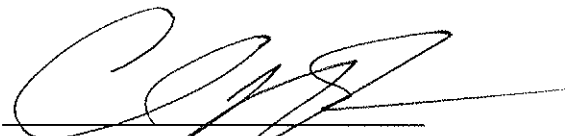


**OFFICE OF COURT ADMINISTRATION**  
**Computer Security Policy for OCA Employees**

**Updated December 14, 2011**

A handwritten signature in black ink, appearing to read 'C. Reynolds', written over a horizontal line.

Carl Reynolds  
Administrative Director

## Introduction

Under the provisions of the Information Resources Management Act, Information Resources are defined as strategic assets of the State of Texas that must be managed as valuable state resources.

The following Computer Security Policies have been adopted:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of Information Resources.
- To preserve the integrity, availability, and confidentiality of Office of Court Administration (OCA) information.
- To ensure protection of OCA Information Resources.
- To educate users of Information Resources about their responsibilities regarding such use.

The Computer Security Policy applies to all OCA employees granted access privileges to OCA Information Resources.

Violation of this policy may result in the removal of Information Resources privileges or disciplinary action up to and including termination.

This administrative policy complies with Texas Administrative Code Title 1, Part 10, Sections 202.1 – 202.28.

## Definitions

**Information Security Officer (ISO):** The appointed OCA management officer responsible for administering/managing data and infrastructure security policy and practice, business continuity, disaster recovery, and the promulgation of security practices and policies.

**Information Resources:** The procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

**Information Resources Manager (IRM):** The director of the Information Services (IS) division; also is the Chief Information Officer for the OCA.

**Portable Computing Device:** Any portable device that is capable of receiving and/or transmitting data to and from OCA

Information Resources. These include, but are not limited to, notebook computers, handheld computers, personal digital assistants (PDAs), pagers, iPads, smart phones, and cell phones.

**User:** An OCA employee who is authorized access to OCA's Information Resources, in accordance with OCA's procedures and rules.

## **Account Management**

In order for a new employee to be given access to OCA Information Resources, the hiring supervisor completes an in-processing form and forwards the form to the Human Resources (HR) Officer. The form is then forwarded by HR to the Service Desk, preferably at least five days in advance of the new employee's start date.

The HR Officer shall notify the Service Desk when an employee is ending employment with the agency; will be on extended leave (more than 30 days); or changes departments or other roles, so that the employee's account can be appropriately managed.

Any changes in an established employee's level of network access during the course of employment will be communicated by the employee's supervisor directly to the Service Desk.

## **Backups**

Backups are run nightly for files residing on the OCA network file servers, email boxes, and databases. Critical files should always be stored on the OCA network file servers, not on the User's computer or User's email account. It is the responsibility of the User to backup any files stored on their computer. Users who need assistance with backups of their computer should contact the Service Desk. Users who wish to recover a file from a backup tape should submit a request to the Service Desk.

Backups are kept in accordance with OCA's record retention policy and are not point in time backups.

## **Business Continuity**

When an employee leaves OCA, their share drive (F: Drive) shall be moved to a location on the server and made available to the person's supervisor or designee for a period of 30 days. After 30 days the folder and its contents shall be deleted. A longer retention period may be requested by the supervisor.

The contents of the User's mailbox shall be archived in the location mentioned above for 30 days. The supervisor may request a longer retention period, and may request that the User's email be delivered to someone else's mailbox. The supervisor shall determine how long to continue the redirection of email.

Assistance in accessing the User's shared drive and/or mailbox is available through the Service Desk.

## **Confidentiality and Non-Disclosure**

Any information that may come to a User's knowledge while using the computer system of OCA or a Texas court shall be held in strictest confidence and may not be disclosed except as authorized by OCA's Administrative Director. The release of such information may be considered a breach of computer security in violation of Section 33.02, Texas Penal Code, and may be prosecuted accordingly.

A User may not disclose the email address of a member of the public unless the member of the public consents to its release, or unless the release is approved by the OCA Administrative Director.

### **Enforcement**

The ISO shall establish procedures (such as automatic lapsing of passwords) designed to enforce and maintain OCA's security policies and procedures.

### **Leaving Your Work Area**

Users must always lock their computer when leaving their work area to prevent unauthorized users from accessing, printing, or downloading data.

### **Malicious Code Protection**

All state-owned computers must be protected by OCA's virus protection software and configuration. Personally owned computers that connect to the OCA network are strongly recommended to have current anti-virus software with up-to-date definitions. Virus protection software on OCA computers must not be intentionally disabled or bypassed.

Any files saved to an OCA computer or network from the Internet or an external device, such as a USB drive, must be scanned for malicious code before opening. Any files suspected of containing malicious code must be cleaned. If a file cannot be cleaned, it must be deleted from the system. Users who need assistance with the scanning or cleaning of files should contact the Service Desk.

### **Network Access**

All remote access to OCA Information Resources must be through an OCA approved means such as Outlook Web Access (OWA), Virtual Private Network (VPN), or other IS applications.

Managers may request a VPN connection for a User by submitting a completed VPN Request Form to the ISO.

Users inside the OCA offices may not be simultaneously connected to the Courts' network and any non-Court network, on the same device.

All connections of the network infrastructure to external third party networks are the responsibility of the OCA IS Division and must be approved by the ISO or IRM.

Dial up or dial back modems at OCA must be preapproved by the ISO or IRM. Users may not divulge dial up or dial back modem phone numbers to anyone outside of OCA.

Unless authorized by the IRM, Users must not download, install or run security programs/utilities that reveal weaknesses in the security of a system (e.g. Users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Courts' network).

Users must not intentionally circumvent the automatic update of security patches on OCA-owned computers.

All OCA equipment connected to the Courts' network must be configured, installed, or changed by the OCA IS Division or by an approved designee of the IS Division. Personally owned computing equipment may only connect to the OCA network through an OCA approved method such as VPN, OWA, or BlackBerry Enterprise Services.

All network infrastructure cabling or network connectivity devices must be installed by the OCA IS Division or by a designee approved in writing by the IRM.

Users may not alter OCA network hardware in any way.

### **Passwords**

All Users of OCA computers or the OCA network must have a personal password, which they must change regularly. If a User suspects their password has been compromised, they must change it immediately. OCA passwords must comply with the following established requirements:

- Password must contain alphabetic, numeric, and special characters
- Minimum password length is set system wide and cannot be changed
- Do not record your password online or send it anywhere via electronic mail
- Do not display your passwords where anyone can see them
- Change your password when requested by the system

If a User forgets their password, they must call the Service Desk to have the password reset. Users may not intentionally circumvent password entry. Exceptions may be made for specific applications with the approval of the ISO or IRM.

Users shall never share their personal password with any other person.

### **Physical Security**

All OCA-managed servers, data communications, and data storage/recovery equipment located at the Capitol Complex are protected in a secure area.

The OCA Facilities Manager is responsible for authorizing access to locked areas within OCA.

Anyone who has not been authorized to enter a secured data center must be accompanied by an authorized OCA employee at all times upon entering the OCA secured data center.

Employees must not give their access badge to anyone.

## **Portable Computing**

The User must take care when storing sensitive or confidential data on a portable computing device. The device must be password protected. The User must exercise reasonable care to ensure the device is kept physically secure.

To ensure that data accessed through a portable computing device is secure, all devices synchronizing with OCA resources are strongly encouraged to utilize the following security features where technically possible:

- A personal identification number (PIN) consisting of at least 4 characters. It is recommended that the PIN be a combination of letters, numbers, and special characters
- The timeout for the PIN should be set to a minimum of 5 minutes.
- A User is allowed 10 attempts to enter the PIN correctly. If the PIN is entered incorrectly 10 times, the device shall be reset to "factory settings" to be unlocked
- Password should be changed periodically, recommended time is every 6 months
- Encryption should be enabled on the device

State-owned portable computing devices are managed according to OCA's Property Management Policy and Property Procedures. Missing, destroyed, or damaged state property must be handled according to these procedures. The User of a state-owned portable computing device must inform the Service Desk immediately of any problems or malfunctions with the equipment.

State-owned portable computing devices should be kept out of direct sunlight, extreme heat, and away from water or environments with damp or humid conditions. Care must also be exercised to prevent physical damage to the device as a result of dropping, crushing, or exposure to powerful magnetic fields (such as are generated by magnets, electrical relay/transmission equipment, etc.).

The User must keep any state-owned portable computing device in his or her custody and may not loan, or otherwise provide the portable computing device to any other person.

The User may not load any software onto a state-owned portable computing device and none of the existing software or configuration options may be altered or deleted, except with prior IS approval.

When available, devices may be checked out from the Service Desk for short periods of time. When a portable computing device is checked out, the Service Desk technician shall maintain a log with property numbers, check-in and check-out dates, and the signature of the individuals using the devices. Portable computing devices that are checked out must be returned to the technician in charge of loaning the portable computing devices. Before returning the portable computing device, the User shall delete all files and data saved on the device.

## **Privacy**

Users have no claim of privacy for any product or communication created, stored, or received by them on any computer equipment owned or operated by OCA. Any such equipment, product

or communication created, stored or received on OCA equipment is subject to audit or inspection at any time without notice.

### **Security Incident Management**

Whenever a User suspects or confirms a security incident has occurred, the User must notify the OCA ISO immediately. The ISO shall coordinate the appropriate response to the incident.

### **Software Licenses**

OCA licensed software or related documentation may not be duplicated unless OCA is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject employees and/or OCA to both civil and criminal penalties under the United States Copyright Act.

Any questions regarding software licensing should be directed to the Software License Manager. The IS Division's Financial Analyst is the designated OCA Software License Manager.

To purchase software, Users must obtain approval from their supervisor or manager and then follow the same procedures OCA uses for the acquisition of other OCA assets. All software acquired by OCA must be purchased through the IS Division to ensure that OCA has a complete record of software, and can support and upgrade such software accordingly. When purchasing software for existing computers, purchases may be charged to the requesting division's budget, or another budget as deemed appropriate by the OCA Administrative Director.

When software is received by OCA, it must be delivered to the Software License Manager for completion of inventory requirements.

All software shall be installed by the IS Division staff. Users shall not install software on OCA computers without authorization from the IRM or ISO. Once installed, the original media (e.g. CDs, DVDs, etc.) shall be kept in a secure storage area maintained by the IS Division.

OCA-owned software may not be installed on a non-OCA computer, unless the software license agreement specifically permits such usage. If a User needs to use OCA-owned software on a non-OCA computer for OCA business purposes, they must complete a Request Form for OCA Software on Personal Computers and seek approval from the appropriate parties. The Software License Manager shall determine if the licenses allow for business use on a non-OCA computer, or if a separate software license needs to be purchased and recorded as an OCA asset. If the User ceases employment with OCA, the User shall remove all OCA software from the non-OCA computer prior to termination.

Users may not load shareware software on OCA's computers, unless approved in writing by the Software License Manager or IRM. Acquisition and registration of shareware products must be handled in the same way as for commercial software products.

Periodic audits of all OCA computers may be conducted to ensure that OCA is in compliance with all software licenses. These audits may be conducted manually or using an automatic auditing tool. The full cooperation of all Users is required during audits.



The IS Division shall remove unauthorized copies of software from OCA owned computers. A User who intentionally makes, acquires, or uses unauthorized copies of software shall be disciplined as appropriate under the circumstance.

### **Training**

To comply with Texas Administrative Code, Title 1, Part 10, Section 202.27(a), OCA requires that all Users are made aware of the agency's computer security policies and procedures, and are provided ongoing information regarding information security requirements and their importance to OCA in terms of agency operations.

OCA's HR Officer shall provide all Users with a copy of this Policy, and shall brief them on the basics of computer security. OCA's ongoing awareness program provides information to agency personnel via electronic mail, the Internet, and presentations. Topics covered in the training include:

- Account Management
- Backups
- Business Continuity
- Email and Internet Use
- Leaving Your Work Area
- Malicious Code Protection
- Misuse of OCA Information Resources
- Network Access
- Passwords Usage and Protection
- Physical Security
- Privacy and Confidentiality
- Security Incident Management
- Software Use and Licensing

All Users must sign an acknowledgment form indicating that they have been informed of and agree to abide by the OCA Computer Security Policy.

The HR Officer shall ensure that each User has read the policy and that each User signs and dates the Acknowledgment Form. The original form is retained by the HR Officer.

# Acknowledgment – Receipt of Information Concerning Computer Security Policy

I, \_\_\_\_\_, acknowledge by my signature below that I  
(Printed Name)  
received a copy of the Computer Security Policy on \_\_\_\_\_, and that I  
(Date)  
shall comply with the Computer Security Policy.

\_\_\_\_\_  
(Employee Signature)

\*\*\*\*\*PLEASE RETURN A COPY OF THIS FORM TO\*\*\*\*\*

THE HUMAN RESOURCES OFFICER