

# UNIFIED JUDICIAL SYSTEM

Policy 213

June 16, 1999

## COMPUTER USAGE

### **SECTION 1.**        **Authority and Purpose**

The purpose of this policy is to establish acceptable terms of use for computers, computer related equipment and other information technology resources.

### **SECTION 2.**        **Computer Use**

All judicial branch owned hardware and software is installed and maintained by the state court information technology department or its designee. Unified judicial system personnel who violate any of these guidelines are subject to disciplinary actions including dismissal.

Microcomputers and peripheral equipment acquired by the ~~Unified Judicial System~~ unified judicial system will only be used for:

1.     Financial administration;
2.     Case information systems.
3.     Legal research;
4.     Word processing;
5.     Development of new or enhancement of existing programs;
6.     Administrative duties;
67.    Other professional activities related to the ~~Unified Judicial System~~ unified judicial system.

This policy does not prohibit the limited use of state-owned computer equipment for non-governmental purposes if all the following requirements are met:

- (a)a. The use does not interfere with the performance of the employee's public duties;
- (b)b. The cost or value related to the use is nominal;
- (c)c. The use does not create the appearance of impropriety;
- d. The use is reasonable in time, duration and frequency;
- e. The use makes minimal use of hardware, software and network resources;
- (d)f. The use is not for a partisan political purposes; and
- (e)g. The use is not for personal commercial purpose.

Only ~~Unified Judicial System~~ unified judicial system justices, judges, and judicial employees and contract employees are authorized, ~~after completing training,~~ to use this judicial branch owned information technology related hardware and systems.

### **SECTION 3. SOFTWARE AND DATA USAGE Software and Data Usage**

The ~~Unified Judicial System~~ unified judicial system has acquired the right to use several proprietary software packages. A license agreement governs the use of the software. ~~Copies of all software license agreements should be filed with the Office of State Court Administrator.~~ People who use the proprietary software should be aware of the agreements between the vendor and the ~~Unified Judicial System~~ unified judicial system. Each person using proprietary software purchased by the unified judicial system is responsible for protecting against any violation of the software license agreements. Typically the agreement states the uses which are NOT permitted, such as:

- making copies of the user's manual;
- making copies of the system ~~diskettes, tapes or other~~ media, unless specifically told to do so in the documentation;
- making alterations to the software source code; OR
- provide use of the software in a multiple CPU or user arrangement to users who are not individually licensed.

Violation of any part of these agreements may create legal and financial liabilities for the ~~Unified Judicial System~~ unified judicial system and the responsible individual(s).

The following conditions govern the use and care of microcomputer hardware and software assigned to the ~~Unified Judicial System staff~~ unified judicial system judges and employees:

- The improper reproduction of proprietary software by any means is prohibited;
- The use of proprietary software which is not the property of the ~~Unified Judicial System~~ unified judicial system on any computing devices belonging to the ~~Unified~~

- ~~Judicial System~~ unified judicial system is prohibited unless authorized to do so in writing by the director of technology;
- The safeguarding of hardware and software assigned is the responsibility of the individual;
  - The staff assigned the proprietary software will abide by the contractual agreements between the vendor of the proprietary software and the ~~Unified Judicial System~~ unified judicial system;
  - Software or other programs shall not be downloaded or installed on judicial system computers. Any unauthorized software found to be installed on a judicial system computer will be removed by state court IT staff.

Data and software which reside on the State's mainframe or agency's mini or microcomputer is the property of the ~~Unified Judicial System~~ unified judicial system or other government agency. Use, alteration or deletion by unauthorized personnel is prohibited. ~~Therefore, Unified Judicial System personnel should not connect Unified Judicial System microcomputers to the State network without written approval from the director of technology. All computer connections to the state network shall be coordinated with the judicial branch information technology department.~~

~~Passwords and identifications used to access the mainframe are confidential and should not be written down and should not be shared unless it expedites the office operations. If the Unified Judicial System personnel have any question regarding these guidelines they should contact the supreme court's director of technology. Unified Judicial System personnel who violate any of these guidelines are subject to disciplinary actions including dismissal.~~

#### **SECTION 4. Security**

1. All workstations shall have automatic screen locking services active with a maximum of a 90-minute activation time.
2. All workstations shall be logged off or have the systems locked when the user leaves the immediate area.
3. Passwords and identifications used to access computer systems are confidential and should not be written down and should not be shared.

Passwords shall:

- a. Contain a minimum of 8 characters;
- b. Contain at least one special character, when supported by the operating

system;

- c. Have a maximum life of 60 days;
- d. Have a minimum life of 6 days;
- e. Not be one of 6 previous passwords used.

4. User Ids

- a. All user IDs shall be disabled after no more than three successive invalid sign on attempts;
- b. No anonymous user IDs will be permitted with the exception of public terminal user IDs.

5. Administrative rights to all computer systems are restricted to judicial branch IT department staff unless an exception is authorized by the director of technology.

**SECTION 5. USE OF THE INTERNET AND REMOTE ACCESS Use of the Internet and Remote Access**

~~The Internet (World Wide Web) is a vast, global network linking computers at sites around the world and it is a vital source for researching and accessing information, communicating through electronic mail (E-mail), and using on-line services.~~

~~Remote Access is a process of connecting via a communication line to the internal state-wide network, which allows connection to the Microsoft NT and Exchange server, AS/400 and the Internet from a remote location.~~

~~Employees are encouraged to become familiar with and use the Internet's and the Remote Access resources to enhance productivity. The state court administrator's office is responsible for controlling the use of the Internet and Remote Access in a reasonable manner to prevent or detect abuse and avoid legal exposure.~~

- 1. Justices, judges and Employees employees of the State Judicial System state judicial system may use the Internet and Remote Access for a purpose related to their employment or official position. An employee may use the Internet and the Remote Access for a non-governmental purposes provided the use if all of the following requirements are met:
  - a. The use does not interfere with the performance of the employee's public duties;
  - b. The cost is of nominal cost or value;

- c. The use does not create the appearance of impropriety;
  - d. The use is not for personal commercial purpose;
  - e. The use is reasonable in time, duration, and frequency; and
  - f. The use makes only minimal use of hardware, ~~and~~ software and network resources.
2. ~~Training. The State Judicial System will offer training for employees on using the Internet and Remote Access so the employees become more informed, knowledgeable, and productive. The training will teach employees how to use the Internet and Remote Access effectively and avoid unlawful use. Training may include software, books, and off-site and in-house training.~~
32. Remote Access. All external connections and remote access to the state network must be requested through the unit court administrator to the state court IT department. External connections will be provided, based on an existing need that addresses the objectives of the judicial branch. Remote Access will be provided within the services readily available and within budgetary constraints. The supervisor's approval is needed in order for Remote Access. In the districts, the Presiding Judge's approval is needed for Remote Access. This may be done in cases where it is necessary to carry out the work of the office or to facilitate the efficient use of equipment or employees. Without the supervisor's approval, a non-exempt employee may not use the Remote Access to work in excess of the standard 40-hour week.
43. Standards of Conduct. An employee's use of the Internet and Remote Access is a privilege, not a right. An employee is solely responsible and shall be personally liable, legally, financially, or otherwise, for the employee's use of the Internet and Remote Access outside the scope of the employee's employment. An employee's use within the scope of employment shall be treated as other activities undertaken by the employee within the scope of employment. An employee's inappropriate conduct may lead to disciplinary action, including restricting the employee's access and use of the Internet or other appropriate action. An employee:
- a. must use the Internet in a professional and ethical manner;
  - b. may not create or distribute immoral, obscene, threatening, defrauding, or violent text or images or transmit inappropriate or unlawful materials through the Internet;
  - c. may not enter or send obscene or offensive material into or through the Internet;
  - d. may not create, distribute, or knowingly use unauthorized copies of

- e. copyrighted material on the Internet;  
must use the Internet only to access files that are publicly available or to which the employee has authorized access;
- f. must refrain from overloading the network with excessive data or wasting computer time, connect time, disc space, printer paper, or other resources;
- g. is responsible for any charges associated with billable Internet services unless appropriate authorization has been obtained prior to accruing the charge;
- h. may not use illegal copies of copyrighted software, store such copies on the State Judicial System computers, or transmit them over the state networks or the Internet;
- i. may be aware that all ~~E-mail~~ email communications maybe subject to disclosure. An employee must not use ~~E-mail~~ email:
  - 1) to harass, intimidate or annoy another person;
  - 2) to send foul, inappropriate, or offensive messages;
  - 3) to solicit outside business ventures; or
  - 4) to send messages that may be interpreted as sexual harassment.

The Judiciary or the executive branch information technology department on behalf of the judiciary may utilize various methods ~~install software~~ to monitor, measure and manage Internet and Remote Access usage. No person may intercept confidential communication except as provided by law.

**SECTION 6.            Antivirus Software**

- 1.    Antivirus software shall be installed and active on all servers and workstations and must be kept current.
- 2.    All incoming files will be scanned for viruses. If a file contains a virus and it cannot be cleaned, the file will be deleted.
- 3.    All files will be scanned on a weekly basis.
- 4.    All log files will be reviewed on a regular basis.
- 5.    Email entering the judicial branch network from the internet will be scanned to detect infected or purposely blocked attachments. All attachments that are infected will be dropped.

6. All servers and workstations will be configured to automatically update and maintain the installed antivirus software using client and workstation management software.
7. Antivirus software shall not be disabled or removed by users.
8. To facilitate automatic updating of the antivirus software, each computer should remain powered on, but logged off at least one night per week, or according to a schedule set by the director of technology.

**SECTION 7. Patch Management**

1. Microsoft critical updates will be installed within 5 days on all workstations utilizing a Microsoft Operating System.
2. Patches and updates will be applied by the state court IT department through the use of client and workstation management software.
3. To facilitate automatic updating of the operating system software, each computer should remain powered on, but logged off at least one night per week, or according to a schedule set by the director of technology.

**SECTION 8. Backup and Recovery**

1. Data in all servers will be backed up nightly, each week night.
2. One back up set per week is stored in a remote location.
3. Testing of the backups will be done periodically.

**SECTION 9. Replacement of Hardware**

1. Each PC, laptop and monitor is replaced according to a four-year replacement cycle and is limited to budgetary constraints. Each year, the oldest one-fourth of the judicial branch computers is targeted for replacement.
2. Printers and citrix computers are replaced on an as-needed basis. The quantity of printers in a given office is dependent on printing volume, number of users and office layout. Sharing of larger, more efficient printers is encouraged.
3. Replaced equipment must be returned to the state court IT department immediately

following successful movement of data and applications to the new computer.

4. Storage devices on replaced equipment are erased.
5. Replaced equipment is sent to Surplus Property for disposal.

**SECTION 10. Email**

1. To facilitate efficient operation and communication within the judicial branch, an email system has been implemented.
2. While limited personal use of the judicial branch email system is not specifically prohibited, the judicial branch email should not be utilized as an individual's primary personal email account.
3. Mail box size limits will be established by the director of technology based on commonly accepted best practices and available storage capacity.
4. The director of technology will maintain a list of email attachments that will be purposely blocked for security reasons. All attachments that are purposely blocked will be removed from the email message. The recipient will receive a message indicating the removal of an attachment. Purposely blocked email attachments will be discarded after 24 hours of their removal.

**SECTION 11. Unsolicited Email (SPAM)**

1. The judicial branch information technology department may employ software or other methods of reducing unsolicited email, realizing that such methods may be imperfect and some legitimate email may occasionally be removed from the email system.
2. Personal email that is removed from the email system by the spam filter will not be forwarded.

Approved by the Supreme Court 02/12/92; amended 06/16/99; amended \_\_\_\_\_