

UNIFIED JUDICIAL SYSTEM

Technology Department Usage Standards

SECTION 1. Security

1. All workstations should have automatic screen locking services active with a maximum of a 90-minute activation time.
2. All workstations should 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 6 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 3 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 2. 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 deleted.
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 computer 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 3. 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 4. Backup and Recovery

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

SECTION 5. Replacement of Hardware

1. Each PC and laptop 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 6 . Email

1. Mail box size limits will be established by the director of technology based on commonly accepted best practices and available storage capacity.
2. 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 48 hours of their removal.

SECTION 7 . 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.