# Automated System Security Guidelines

## <u>DATA SECURITY</u>

Each user of an OSCA-supported network with access to sensitive information shall receive a copy of these guidelines upon employment or start of contract. Outside consultants, contractors, and temporaries shall be subject to the same security requirements and have the same security responsibilities as court employees.

### 1. Information Sensitivity Levels

### 1.1. Level 1 -- Open Information

Open Information includes all information that is not otherwise classified in sections 1.2 through 1.5. This information is <u>not sensitive</u> and is open to the public.

NOTE: Due to limitations in the public access system (*CaseNet*), cases are classified as level 2 if only part of the case information is Open Information.

1.1.1. Open information includes, but is not limited to:

- party and case header information on cases transferred to the Prosecuting Attorney awaiting verdicts, and
- party and judgment information on closed paternity cases.

### 1.2. Level 2 -- Private Information

Private Information includes individual or employee private information and computer documentation. Its unauthorized disclosure could adversely impact the judicial system. Access to Private information shall be controlled on a need-to-know basis.

### 1.2.1. Individual Private Information

1.2.1.1. Individual private information includes:

- social security number,
- home address and telephone number,
- place of employment, and
- private information of related parties (spouse, children, etc.).

1.2.1.2. Court employees may release the private information directly linked to a specific individual to third parties if:

- the individual provided prior written consent, or
- the law requires the disclosure.

1.2.1.3. Court employees may disclose statistical information derived from individual records to third parties if the information cannot identify the specific persons.

### 1.2.2. Employee Private Information

1.2.2.1. Employee private information includes:

- home address and telephone number, unless waived by the individual,
- performance reports,
- background investigation results,
- information regarding ongoing security investigations,
- drug tests results, and
- reason for termination.

1.2.2.2. Employee private information shall not be given to third parties without the permission of the employee unless required by law.

1.2.2.3. Employees shall be permitted to both examine and make copies of their own personal information except the security investigation documentation that shall be disclosed after the investigation has been completed.

### 1.2.3. Computer Documentation

1.2.3.1. Computer documentation includes:

- the physical address of the computer center,
- alarm authentication cards and codes for buildings housing computers,
- the internal addresses, configuration, and system design information for networked computers,
- system controls in use and how they are implemented,
- information about the location of sensitive data,
- the methods of accessing the computer system, such as dial-up modem phone numbers,
- specific methods used to exploit system vulnerabilities, and
- information about the individuals, organizations, or specific systems damaged by computer crimes.

1.2.3.2. OSCA-supported network users shall not disclose computer documentation to third parties without the advance written permission of the Information Technology Division Director. Disclosure of electronic mail addresses, however, does not require permission.

### 1.3. Level 3 -- Confidential Information

1.3.1. The Confidential sensitivity classification applies to most closed (not publicly disseminated) information as required by Missouri state law and Supreme Court Administrative Rules. It may be disclosed to court employees and other persons according to these statutes and rules. Its unauthorized disclosure would adversely impact the Missouri system, individual persons and the public. Confidential Information includes:

Case Types:

- Paternity (open cases only. Party and judgment information on closed paternity cases is private/level 2)
- Grand jury proceedings

Disposition Types:

- Nolle pros
- Dismissed (except civil)
- Not guilty verdicts
- Suspended imposition of sentence (following successful completion of probation)

Documents:

- Sexual offender registration, photographs and fingerprints
- Driver's Risk Inventory (DRI)
- SATOP offender assignment forms AA and C
- Appeals court settlement schedules
- Presentence investigations, probation reports, parole reports
- Documents regarding artificial insemination

Party Data:

- Identity of applicants for or recipients of state public assistance or welfare (including IV-D child support)
- Medical or disability information
- Data by attorney

1.3.2. All third party proprietary information entrusted to the judicial system shall be treated as though it was confidential information unless specified otherwise by contract.

### 1.4. Level 4 -- Juvenile, Mental Health and Drug Abuse Information

Missouri state law and the Supreme Court Administrative Rules require Juvenile, Mental Health, and Drug Abuse Information to be kept from the public and from court employees who do not have a need to know. It may be disclosed according to these statutes and rules. Its unauthorized disclosure would seriously impact the Missouri system, individual persons and the public. Juvenile, Mental Health and Drug Abuse Information includes:

- juvenile cases which are not sealed,
- adoption cases,
- mental health cases, to include criminal mental health evaluations if the person pled not guilty by reason of mental disease or defect,
- alcohol or drug abuse cases, to include court-ordered HIV testing results, and
- confidential appellate cases

### 1.5. Level 5 -- Sealed Information

Sealed Information is the most sensitive information within the judicial system and must be protected as required to by Missouri state law and Supreme Court Administrative Rules. It may be disclosed to specified individuals only according to these statutes and rules. Its unauthorized disclosure could severely impact the Missouri judicial system, individual persons and the public. Sealed Information includes:

- any case ordered sealed.
- grand jury indictments (until served).
- search warrants

## 2. Handling Sensitive Information

Court employees shall protect information in a manner commensurate with its sensitivity, value, and criticality.

### 2.1. Disclosure

2.1.1. All access to sensitive information is restricted based on the need-to-know and granted only by a clear chain of authority delegated from the information owner.

2.1.2. All court employees, consultants, contractors, and temporaries shall sign a confidentiality agreement at the time they enter the system.

2.1.3. All disclosure of level 3 through level 5 information to third parties shall include a signed non-disclosure agreement. The agreement shall include:

- a description of the disclosed information,
- restrictions on its subsequent dissemination,
- a statement of how the third party may and may not use the information, and
- specifications on how to audit the security controls.

2.1.4. If an employee, consultant, agent, or contractor receives level 3 through level 5 information from a third party on behalf of the judicial branch, the third party shall sign a release form.

### 2.2. Labeling

2.2.1. All sensitive information from level 3 through level 5 shall have an appropriate label indicating its sensitivity level regardless of the storage media, the storage location, the computer system, or the handling processes used. It shall retain this label during its entire existence, from creation to destruction or declassification.  Open and Private information (levels 1 and 2) do not need labels.

2.2.2.  When information of various sensitivity levels is combined into one document, the new document shall be labeled with the highest sensitivity level found in the original sources.

2.2.3.  Sensitivity labels shall stand out from the rest of the text by color (red is preferred), bolding, larger print size, or set off by asterisks on either side.

### 2.3.  Copying and Printing

2.3.1.  Employees shall restrict the number of copy machine or printed copies of level 3 through level 5 information to the minimum number required.

2.3.2.  Employees shall not leave printers unsecured if level 3 through level 5 information is being or soon will be printed.  The persons attending the printer shall have authorized access to the information being printed.  Printing may be unattended if physical access controls prevent unauthorized persons from viewing the material being printed.

2.3.3.  If a copy machine or printer jams while producing level 3 through level 5 information, the employee shall not leave the machine until he removes or destroys the copies.

### 2.4.  Mailing and Transporting

2.4.1.  Employees shall ship or mail level 3 through level 5 information in a sealed opaque envelope marked "Open by Addressee Only".  Registered mail with a return signature is preferred.

2.4.2.  Employees shall personally deliver level 3 through level 5 computer or fax output to the designated recipients.  This information shall not be left on an unattended desk or in an unoccupied office.

2.4.3.  Hardcopy or unencrypted magnetic media containing level 3 through level 5 information being taken outside the court premises shall be not be left unattended except in a locked and alarmed facility.

2.4.4.  Transportable computers such as portables, laptops, notebooks, palmtops, etc. containing level 3 through level 5 information shall not be left unattended or in a non-alarmed facility unless the data has been encrypted.

2.4.5.  Computers shall not be checked in to airline luggage systems, but shall remain in the possession of the traveler as a carry on, if possible.

2.4.6.  A log shall be kept whenever level 3 through level 5 information is removed from the court premises.  The log shall record the date, the information involved, and the persons removing the information.

### 2.5.  Electronically Transmitting

2.5.1.  OSCA-supported network users shall encrypt level 3 through level 5 information sent over any communication network including an electronic mail system by an encryption method approved by the Director of the Information Technology Division.

2.5.2.  Before computer system users transfer any level 3 through level 5 information from one computer to another, they shall ensure that access controls on the destination computer are at least as secure as those on the sending computer.

2.5.3. Prior to distributing any electronic media to third parties, court users shall first scan it for viruses.

2.5.4. Before transmitting level 3 through level 5 information by fax, the employee shall first receive assurance from the recipient that an authorized person is present at the destination fax machine or that the area surrounding the receiving fax machine is in a restricted area which prevents unauthorized access.

2.5.5. Employees shall not fax level 3 through level 5 information via untrusted intermediaries (hotel staff, staff of a rented mailbox store, etc.).

2.5.6. All outgoing faxes shall include an approved cover sheet giving the sensitivity level of the fax (if level 3 through level 5) and a person and phone number to contact in the event of mis-routing.

### 2.6. Sensitive Discussions

2.6.1. Employees shall not read, discuss, or otherwise expose level 3 through level 5 information on airplanes, in restaurants, or other public places.

2.6.2. Persons other than those specifically invited shall not attend meetings involving the discussion of level 3 through level 5 information.

2.6.3. All meetings with third party visitors not authorized access to level 3 through level 5 information shall take place in fully enclosed rooms, void of sensitive materials and separated from sensitive work in progress.

2.6.4. Any speaker orally disclosing level 3 through level 5 information in a meeting, seminar, lecture, or related presentation shall clearly communicate the sensitivity of the information. The speaker shall also remind the audience to use discretion when disclosing it to others. Visual aids such as slides and overhead transparencies shall include the appropriate sensitivity labels.

### 2.7. Storing

2.7.1. The maximum amount of time a employee may leave level 3 through level 5 information in an unattended or unalarmed but locked facility is thirty (30) minutes. If the employee will be away more than thirty minutes, he shall lock the material in appropriate furniture.

2.7.2. Users shall log-out or lock with a screen-saver password any computer connected to a network or containing sensitive (level 2 through level 5), critical, or valuable information on its hard drive when leaving the machine unattended. This is particularly important on PCs with modems that do not have additional access controls.

2.7.3. Users shall always secure level 3 through level 5 information at the end of the workday, preferably by locking it in file cabinets, desks, safes or other furniture in a facility that is alarmed during non-working hours. If the information is protected by an approved encryption system, however, it need not be in a locked container.

2.7.4. If level 3 through level 5 information is currently in use, it shall be kept clearly visible to authorized persons and kept out of sight of unauthorized persons.

2.7.5. Court computer users shall encrypt and/or use a password to protect level 3 through level 5 data stored on workstations, laptops and computer-readable storage media (such as magnetic tapes, floppy disks, or CD-ROMs).

### 2.8. Back-Up

2.8.1. OSCA-supported network users shall store sensitive, critical or valuable information on the server rather than their own local hard drives (usually the C drive) to ensure proper back-ups are made.

### 2.9. Downgrading and Destruction

2.9.1. Before sending computer magnetic storage media to a vendor for servicing, trade-in, or disposal, computer system users shall destroy or conceal all sensitive information according to methods approved by the State Judicial Records Committee.

2.9.2. All recording media such as dictation tapes, tape recorder tapes, or similar media containing level 3 through level 5 information shall be erased as soon as possible.

2.9.3. Employees shall place all level 3 through level 5 information ready for destruction--no matter what forms it takes (disk, hardcopy, etc.)--in designated secure containers until destruction.

2.9.4. Materials that unauthorized persons could analyze to deduce sensitive information shall be destroyed in the same manner prescribed for destroying actual sensitive information. This policy includes printer and typewriter ribbons, carbon papers, mimeograph stencil masters, photographic negatives, aborted computer hardcopy output, unacceptable photocopies, and so forth.

2.9.5. OSCA-supported network users shall not destroy potentially important information without advance management approval. Employees shall retain information if:

- it will likely be needed in the future,
- regulation or statute requires its retention (see Administrative Rule 8), or
- it will likely be needed in the investigation or prosecution of unauthorized, illegal, or abusive acts.

## 3. Intellectual Property Rights and Copyrights

3.1. The programs and documentation generated by court employees, consultants, or contractors for the benefit of the court computer system are the property of the judicial branch. Specific exceptions shall be in writing.

3.2. OSCA-supported network users shall not make unauthorized copies of software. The judicial branch strongly supports strict adherence to software vendors' license agreements and copyright holders' notices.

3.3. Employees shall not copy software programs provided by the judicial system to any storage media (floppy disk, magnetic tape, etc.), to another computer, or distribute them to outside parties without written permission from the Director of the Information Technology Division.

3.4. All court employees or persons who place information in the public area of electronic bulletin board systems (BBSs) or Web sites, grant to the judicial branch the right to edit, copy, republish, and distribute such information.

## 4. Access Controls

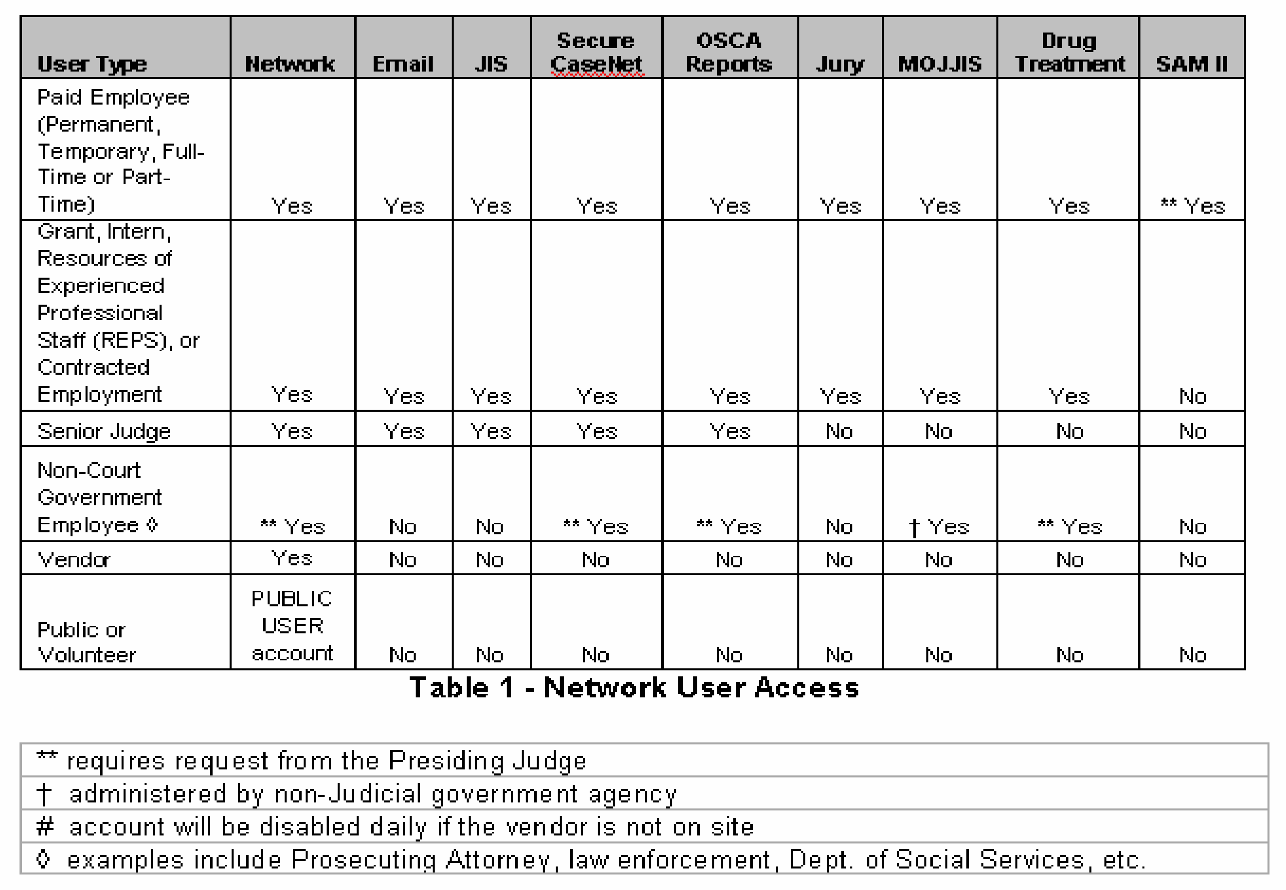
4.1. OSCA-supported network users shall comply with the control requirements specified by the owner and custodian of the information.

4.2. All OSCA-supported network users shall have a unique userid and password to gain access to the shared network. Exceptions may be generic userids used for inquiry only, such as the public access terminals, and generic userids for high-turnover positions (such as interns). A log must be kept of who is using the generic userid at any one time for high-turnover positions. All userids must be deleted upon employment termination.

4.2.1. All requests for user access to the judicial network shall be submitted by the Appointing Authority or their delegate, and submitted at least 2 working days prior to the needed access. The Security Requests database is available through Lotus Notes to use for most state-wide systems security issues.

4.2.2 All judicial network users who are not court employees (i.e., all contractors, non-paid interns, etc.) shall sign a non-disclosure agreement before obtaining access to the court network.

4.2.3 Access to the judicial network and state-wide court applications may be granted according to Table 1 – Network User Access. Specific permissions for each application (such as the ability to print checks or create a report) shall be detailed in the security request referred to on paragraph 4.2.1.



| User Type | Network | Email | JIS | Secure CaseNet | OSCA Reports | Jury | MOJJIS | Drug Treatment | SAM II |
|---|---|---|---|---|---|---|---|---|---|
| Paid Employee (Permanent, Temporary, Full-Time or Part-Time) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | ** Yes |
| Grant, Intern, Resources of Experienced Professional Staff (REPS), or Contracted Employment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Senior Judge | Yes | Yes | Yes | Yes | Yes | No | No | No | No |
| Non-Court Government Employee ◊ | ** Yes | No | No | ** Yes | ** Yes | No | † Yes | ** Yes | No |
| Vendor | Yes | No | No | No | No | No | No | No | No |
| Public or Volunteer | PUBLIC USER account | No | No | No | No | No | No | No | No |

Table 1 - Network User Access

| | |
|---|---|
| ** | requires request from the Presiding Judge |
| † | administered by non-Judicial government agency |
| # | account will be disabled daily if the vendor is not on site |
| ◊ | examples include Prosecuting Attorney, law enforcement, Dept. of Social Services, etc. |

4.2.4. Network User Access that are not covered in Table 1 shall be requested in writing to the Missouri Court Automation Technical Access Policy Task Team by the Presiding Judge.

4.2.5. All equipment on the judicial network shall be court-controlled.

4.3. OSCA-supported network users shall be held responsible for all activity performed with their personal user-IDs. They shall not use any user-ID other than the one issued to them and shall not allow others to use it.

4.4. Any request for additions or changes (except deletions) to user security shall be authenticated. This may be by signed messages or email, by the technician initiating the conversation to the requestor, or by voice recognition as a last resort. Security requests initiated by the requestor via telephone require a call back to the requestor using a published phone number (not one provided by the requestor). The Security Requests database is available through Lotus Notes for appointing authorities and/or their designees to use for most state-wide systems security issues.

4.5. OSCA-supported network users shall not disclose any of their passwords to anyone, inlcuding their supervisors. If computer system users need to share data, they shall use access control lists, electronic mail, public directories on local area network servers, and other approved mechanisms.

4.6 If a technician must assume another user's identity to perform maintenance, the technician shall make a log of the use of the id and the reason for its use in the Help Desk system. When the technician is finished, the password shall be reset and shall be required to be changed at the user's next logon.

4.7. Users shall promptly change all passwords if they suspect or know unauthorized parties received the passwords.

4.8. Users shall not write down their passwords unless they have a secure method of storing them, such as saving them in an encrypted file or storing them in a locked safe.

4.9. Passwords shall <u>not</u> be:

- the default password assigned by the system administrator,
- related to the job or personal life, e.g., not a license plate number, spouse's name, address, telephone number, etc.,
- words, i.e., not proper names, places, or slang,
- a certain number of characters that do <u>not</u> change combined with a certain number of characters that <u>predictably</u> change. In these prohibited passwords, users typically base characters that change on the month, division, project, or some other easily guessed factor. For example, users may not choose passwords like "X34JAN" in January, "X34FEB" in February, etc., or
- identical or substantially similar to passwords the user previously chose.

Passwords shall be:

- be hard to guess,
- contain at least one alphabetic (a-z) and one non-alphabetic (number or punctuation) character,
- contain at least one lower case and one upper case alphabetic character,
- contain at least 8 characters total,
- be changed on a periodic basis commensurate with the sensitivity, criticality and value of the information it protects, and
- be different for each application or network the user logs on to unless the computer system contains single sign on software.

4.10. If an identification badge, physical access card, or system access token (smart card, telephone credit card, etc.) is lost or stolen, or suspected of being lost or stolen, the employee shall report the loss to the appropriate security manager immediately.

4.11. Modification to an Access Control List (ACL) of an OSCA-supported employee's personal data file or email stored on OSCA-supported equipment may be requested by the employee's supervisor, and authorized by the employee's appointing authority, Chief Justice, Court Administrator, or State Court Administrator. Supervisors may share their personal network folder with subordinates only if they retain a sub-folder which is not shared with any subordinates. The request and authorization must be on official letterhead or via signed email and sent to the OSCA Systems Security Office. Such modifications shall be documented and shall expire yearly. Information Technology Technicians, under the guidance of the Missouri Judiciary, shall have the minimum access to user data files and email required to perform their duties.

## 5. Unauthorized Use of Systems

5.1. Unauthorized use of the OSCA-supported network is strictly prohibited and may be subject to criminal prosecution or employee discipline. Authorized personnel may monitor any activity or communication on the system and may retrieve any information stored within the system. By accessing and using the computer, users are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with the unit (e.g., floppy disks, PDAs and other hand-held peripherals, CD-ROMs, etc.).

5.2. Users shall not interfere with the proper operation of computer and communications systems, adversely affect the ability of others to use these systems, or conduct themselves in a manner that is harmful or offensive to others. These systems are private and not public forums, and as such, do not provide First Amendment free speech guarantees. Harassment--including unwanted telephone calls, electronic mail, faxes, and internal mail--should not be tolerated on any judicial systems. Management maintains the authority to:

- restrict or revoke the privileges of any user at any time,
- inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine security, and
- take any steps necessary to manage and protect its computer and communications systems. Management may exercise this authority with or without notice to computer system users.

5.3. OSCA-supported network users shall not attempt to compromise internal controls, obtain resources beyond those authorized, gain access to systems without proper authorization, or exploit vulnerabilities or deficiencies in the security of systems unless specifically approved in advance by the Director of the Information Technology Division. Users shall promptly report all vulnerabilities and deficiencies they discover to the Director of Information Technology or the Systems Security Officer.

5.4. Court electronic mail, fax machines, voice systems, or any other communications systems shall be used only for official business unless authorized by the individual's supervisor.

5.5. Computer system users shall not run any computer program that would unduly consume more computer resources than necessary for performing official work.

5.6. Users shall not store or use games on any systems without the approval of their supervisor.

5.7. On occasion, it may be necessary for OSCA support staff to access another user's computer through the use of Microsoft Systems Management Server (SMS). The OSCA support person using SMS to take control of the user desktop and thereby assume the user's network identity, will only do so with proper consent from the user or the user's direct supervisor. The OSCA support person shall remain on the telephone with the user during the entire event unless the user has provided written authorization (e-mail or hardcopy). If the user states he or she must leave the PC for any reason, the OSCA support person shall close the remote session until the user returns, unless written permission to remain connected has been provided. Remote help management connection permission, either verbal or written, shall be documented in the Help Desk ticket.

5.8. SMS is capable of, and the preferred method for large scale software deployments. Automated/unattended software packages will be assembled and tested by Systems Operations staff prior to deployment. Only authorized OSCA Systems Operations staff or designees will create and advertise the packages for installation by SMS after contact has been made with each site regarding the upcoming installation.

## 6. Electronic Mail (Email)

6.1. Electronic mail systems are primarily for official purposes. Any personal use shall not interfere with normal activities, involve solicitation, or for-profit outside business activity, shall not potentially embarrass the judicial system and shall be approved by the individual's supervisor.

6.2. Management, supervisors and system administrators may read electronic mail messages to correct problems with the system or perform other functions of their jobs. Thus, email is not totally private and the contents of email messages may be read without prior notice to the user. Users shall have no expectation of privacy. If it is discovered that a user may be conducting unauthorized activities using the electronic mail system (those specifically proscribed by OSCA policies and procedures or federal or state statutes and regulations), disciplinary action may be taken. Evidence of criminal wrongdoing may be disclosed to law enforcement officials. Individuals using the email system for a purposes other than judicial business, do so with the agreement that they waive their right to privacy for any messages sent or received.

6.3. OSCA-supported network users shall encrypt electronic mail messages containing sensitive information (level 2 through level 5). All electronic mail messages and files shall be treated as private and direct communication between a sender and a recipient. However, users shall remember that electronic mail that is not encrypted is the electronic equivalent of a postcard written in pencil.

6.4. Each user shall use his own user-ID and password to access electronic mail. Users shall not masquerade as other individuals via electronic mail.

6.5. Access to an OSCA-supported employee's personal data file or email stored on OSCA-supported equipment will be allowed as outlined in section 4.11

6.6. All copies of email ID files will be deleted as soon as it is feasible, i.e., after initial installation, after employee is terminated, after trouble-shooting a Help Desk call, etc. Only the copies of the ID file in use by the end user and in the Judicial IDs & Certificates database will be retained.

6.7. All buttons in the body of email messages must be signed.

## 7. Internet and Outside Network Connections

7.1. Users shall not establish direct external network connections (Internet or otherwise) without prior approval of the Director of Information Technology. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet FTP servers, and the like.

7.2. Users shall not establish any communications systems that accept in-coming dial-up calls, modem connections, electronic bulletin boards, local area networks, or other multi-user systems without the specific approval of the Director of the Information Technology Division.

7.3. Users connecting to an OSCA-supported network from an external network such as the Internet shall authenticate themselves at a firewall before gaining access. The authentication shall be via an extended user authentication process (such as SecurID tokens, smart cards, user-transparent challenge and response systems, or full session encryption) approved by the Director of Information Technology.

7.4. All approved dial-up modems shall not answer in-coming calls until the fourth ring. This will thwart people seeking to gain unauthorized access using programs that identify telephone lines connected to computers.

7.5. Users shall not continually leave approved dial-up modems connected to PCs in the auto answer mode, that is, always able to receive in-coming dial-up calls, without approval from the Director of Information Technology.

7.6. Users shall avoid simultaneously connecting their workstations to an OSCA-supported network and an approved dial-up modem or the Internet.

7.7. Users shall not place material (software, internal memos, press releases, etc.) on any publicly accessible Internet computer system unless the posting has first been approved by the information owner.

7.8. OSCA-supported network users shall not send sensitive information (level 2 through level 5), credit card numbers, proprietary software, or log-in passwords via the Internet unless it has first been encrypted by approved methods.

7.9. Before court employees release any internal information, enter into any contracts, or order any products via public networks (the Internet), they shall confirm the identity of the individuals and organizations contacted. It is relatively easy to spoof the identity of another user on public networks. Ideally, identity confirmation is performed via digital signatures, but in cases where these are not available, they may use other means such as letters of credit, third party references, and telephone conversations.

7.10. Supervisors shall provide guidance on a subordinate’s use of court computer systems to access the Internet for personal purposes.

7.11 All proposed connections between the judicial network and any other network shall be requested in writing to the Missouri Court Automation Technical Access Policy Task Team by the Presiding Judge.

## 8. Externally Supplied Software, Hardware and Storage Media

8.1. OSCA-supported network users down-loading files and software via the Internet (or any other public network) or installing authorized diskettes or CDs received from outside the judicial system shall:

- log-out of all file servers and terminate all other network connections,

- decompress all externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) prior to the virus check. Many virus checking programs cannot detect viruses in compressed files,
- screen the software with an approved virus detection package before executing the software, i.e., prior to being run or examined via another program such as a word processing package, and
- if screening detects a virus, the user shall immediately notify the Information Technology Division or Systems Security Officer and stop all work on the workstation.

8.2. OSCA-supported network users shall not bring their own computers, computer peripherals, or computer software into facilities or connect them to the network remotely without prior authorization from the Information Technology Division.

8.3. OSCA-supported network users shall not install executable software or modify existing software on equipment without first obtaining approval from the Information Technology Division. Many products over-burden system resources (such as Web Shots screen savers) or are not compatible with existing software.

8.4. All software that handles sensitive (level 2 through level 5), critical, or valuable information shall obtain approval from the Information Technology Division prior to being used for production processing.

8.5. OSCA-supported network users shall not intentionally introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of computer memory, file system, or software. This includes viruses, bacteria, worms, Trojan horses, and any other harmful software.

8.6. OSCA-supported network users shall not install hardware or software that unauthorized persons could use to evaluate or compromise system security without specific authorization from the Information Technology Division. Such tools include those which defeat software copy-protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

## 9. Remote Access Service (RAS)

9.1. Remote access arrangements are at the discretion of the supervisor and are limited to only those users whose jobs require remote access. Before RAS is approved, the remote working environment shall be in compliance with policies and standards for physical security as well as having approval from the Director of Information Technology.

9.2. Users with RAS shall agree to abide by all system security procedures. These include, but are not limited to, compliance with software license agreements, avoiding simultaneous connections to an OSCA-supported network and the Internet, performing regular back-ups, not leaving the modem on and in auto answer mode, and using approved destruction methods to dispose of level 3 through level 5 information.

9.3. RAS shall be installed only on court owned or managed equipment.

9.4. Users connecting to an OSCA-supported network from an external network such as a public phone line shall authenticate themselves via an extended user authentication process (such as SecurID tokens, smart cards, user-transparent challenge and response systems, or full session encryption) approved by the Director of Information Technology.

9.5. Users shall not store their SecurID token, smart card, etc. with their laptop computers.

9.6. RAS shall be used for job related duties. RAS shall not replace users' personal Internet Service Provider or personal email.

9.7. Management, supervisors and system administrators may read electronic documents transmitted via RAS to correct problems with the system or perform other functions of their jobs. Thus, RAS is not totally private and the contents of RAS transmissions may be read without prior notice to the user. This policy also applies to password-protected communications. However, access to password-protected communications without the consent of the sender or recipient requires prior approval from the State Courts Administrator.

9.8. If it is discovered that a user may be conducting unauthorized activities using RAS (those specifically proscribed by OSCA policies and procedures or federal or state statutes and regulations), disciplinary action may be taken, up to and including, dismissal. Evidence of criminal wrongdoing may be disclosed to law enforcement officials. Individuals using RAS do so with the agreement that they waive their right to privacy for any documents sent or received.

9.9. The RAS telephone numbers are confidential and may not be disclosed to unauthorized individuals.

9.10. All OSCA-supported network users who keep sensitive information (level 3 through level 5) at their homes shall store it in lockable furniture.

## 10. Physical Security of Computer Assets

10.1. Computer centers shall be closed shops. Users inside computer centers shall not allow others to enter computer the centers without authorization from the Director of the Information Technology Division or the Systems Security Officer.

10.2. Only those whose job responsibilities require their presence shall have access to the magnetic tape, disk, and documentation libraries within the computer center.

10.3. No one shall smoke, drink from anything but a spill-proof cup, or eat in the computer room.

10.4. Computers (including laptops), printers, modems, and related equipment shall not leave premises unless accompanied by an approved property tag.

10.5. Users shall not alter computer equipment provided in any way (e.g., upgrade the processor, expand the memory, add a modem, or insert an extra circuit board) without the equipment owner's authorization

10.6. Users shall not move or relocate microcomputer equipment (PCs, LAN servers, etc.) without the prior approval of the involved system administrator and inventory control administrator.

10.7. All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs) containing sensitive information shall be physically secure when not in use. The only exception is when an approved encryption system protects the information.

10.8. Users shall position computer screens which process sensitive information so that unauthorized persons cannot see the data on the screen from public counters, windows or doorways.

## 11. Security Incidents and Violations

11.1. Users shall report all suspected security incidents, violations, software malfunctions, vulnerabilities, discrepancies, disruptions of operations, or problems as quickly as possible to the Information Technology Division or the Systems Security Officer. A security incident is the suspected or known loss or unauthorized disclosure of sensitive data to unauthorized parties. A security violation is the failure to follow approved security procedures.

11.2. Each judicial information system user is responsible for security on a day-to-day basis. Security is NOT solely the responsibility of the Information Technology Division or the Systems Security Officer.

11.3. Minor security violations are such things as using a weak password, failing to label sensitive information or installing unauthorized software. Examples of major security violations are connecting an OSCA-supported network computer to an untrusted outside network without approval or selling level 4 or level 5 information to an unauthorized third party.

11.4 If an OSCA-supported network user suspects infection by a computer virus or other harmful software, he should:

- immediately stop using the involved computer,
- write down the file involved and commands just executed, and
- notify the LAN administrator, the Information Technology Division and the Systems Security Officer.

## 12. Termination or Suspension of Accesses

12.1. Individuals leaving employment or terminating a contract shall inform their supervisor about all property they possess, as well as all computer system privileges, building access privileges, and other privileges they have. Supervisors shall ensure all accesses and privileges are removed as soon as they are no longer needed. Examples of these accesses and privileges include, but are not limited to, RAS tokens, identification cards, building access cards, alarm access cards and keys.

12.2. Supervisors shall immediately terminate the accesses of all OSCA-supported network users who have stolen property, acted with insubordination, or been convicted of a felony. Supervisors shall escort the individual while he collects and removes his personal effects until he exits the premises.

12.3. Supervisors of all involuntarily terminated computer support personnel shall immediately relieve these users of all of duties, ensure they return all equipment and information, and escort them while they pack up their belongings and exit premises.

12.4. A supervisor shall suspend all accesses and privileges if he suspects the employee of a security breach requiring an extended investigation. The supervisor may disclose the reason for the suspension to other OSCA-supported network users only after obtaining permission from the Director of the Information Technology Division.