UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

COMPUTER SECURITY MANUAL

Automation Usage and Security Procedures

The purpose of this document is to acquaint automation users with automation usage and security practices required by the Administrative Office of the United States Courts (AO).

Whereas, staff is the first and best line of protection from compromise of data on the various computer systems, all chambers and clerk's office users are responsible for applying the concepts and policies in this document while performing the tasks that relate to their jobs.

Passwords

Sensitive and confidential information require protection from disclosure, alteration and loss. An important part of this protection is through password protection.

The password policy is as follows:

- Novell passwords must be at least seven characters and must contain at least one non-alphanumeric character; they must not be all alphabetic characters. Novell passwords must be changed every 90 days. The network will automatically notify and prompt users when it is time to change Novell passwords.

  SAMPLE: **wt29?mp**

- Lotus Notes e-mail passwords have the same requirements as Novell passwords: a minimum of 7 characters including at least one non-alphanumeric character. The passwords expire every 180 days with a grace login period of 15 days. Users will be informed of the expiration and asked to change their password. These requirements also apply to the Lotus Notes Internet password. Lotus notes will also determine the “strength” of your password and, if it is not “strong” enough, you will be prompted to choose a different password.

- Lotus Organizer Passwords, if used, may be the same as the Lotus Notes password.

- CM/ECF and CHASER passwords must be at least seven characters and must contain one numeric character. CM/ECF and CHASER passwords must be changed every 90 days. The computer will automatically prompt users when it is time to change CM/ECF and CHASER passwords.

  SAMPLE: **xu29pwq**

- Users may not use Novell and CM/ECF passwords that are identical.

- Passwords may not be single, meaningful words (words found in a dictionary), family names, birthdays, nicknames, place names or simple alphanumeric sets like"WXYZ" or "2468".

- Passwords may not be a user's name or login name.

- Passwords may not be a name or word with the order of the letters reversed.

- Passwords may not consist of a single, meaningful word with a number following it.

- Passwords may not be changed by merely adding or increasing a number.

- If passwords are "rotated," use at least 5 different passwords.

- Passwords <u>must not</u> be written down, posted in work areas, shared with others (including IT staff) unless required for relief coverage.

If you suspect a breach of security, change your password immediately and notify the IT department for assistance.

Passwords are monitored by IT for compliance with this policy.

Automation Usage and Security Procedures

Protection of Data Files and Court Information

The policy regarding protection of data files and court information is as follows:

- Make a back-up copy of all important files. Making back-up copies of important computer files is the single most important action to protect information from loss or unauthorized modification.

- If data is stored on the network, it will be automatically backed-up on a daily basis. It is recommended that sensitive and important documents stored on the network also be backed-up to the hard disk (C: drive). This provides security and access to the data in the event the network is not available.

- It is strongly recommended that users do not work from floppy disks. Copy files to the network (H: or S: drives), retrieve and modify the document, re-save it with the changes, and then copy the revised document back to the floppy disk. This will ensure that the data is stored in a secure manner.

- Protect sensitive data; printouts and program documentation with sensitive information should not left in plain sight. Sensitive information can be described as names, addresses, social security numbers and other information that can lead to identity theft. Budget and accounting material, benefit information and salary data, sealed cases, juvenile cases and draft legal opinions should also be considered as sensitive information. Any media used to store the information, whether it is paper, internal hard disks, external disks, Zip disks, CDs, DVDs, USB storage devices is susceptible to theft and should be password protected when possible.

- Teleworkers have the added responsibility of protecting judiciary information in a temporary work space, which can be a less secure environment than an office. The Court's telework policy states that teleworkers are responsible for the security and protection of all government records and data against unauthorized disclosure.

- Protect data; external storage devices left out and/or unlabeled may be picked up and used by others.

Immediately report loss of data or court information to the IT department for assistance.

Software Policies

The software policy is as follows:

- In accordance with General Order No. 96-8, no personal software may be installed by a user on a court computer unless the software is approved, purchased and installed by the IT department.

- All copyright laws, regulations and policies will be strictly enforced; no outside software will be loaded without the prior authorization of the IT department.

- All standard computer configurations will be in compliance with the AO guidelines. Requests to modify the standard configurations due to unique needs must be directed to the IT department.

- The IT department will maintain an updated list of all software currently under license for the Court.

Copyright and License Agreements

Software copyright and license agreements exist on almost all commercial software products:

- Do not bring unauthorized or personal software to work.

- Unauthorized reproduction of copyrighted software or documentation is against the law.

- Penalties for violation of copyright and license agreements include compensatory damages levied up to $100,000 per unauthorized copy and, under certain circumstances, individuals can be sentenced to up to five years in prison and fined $250,000.

Automation Usage and Security Procedures

Internet and Intranet Access

The Internet and Intranet policies are as follows:

- Internet access is authorized for all district and magistrate judges, and judicial staff as approved by their respective judge. Internet access is authorized for clerk's office staff as approved by the Clerk of Court.

- Use of the Internet services provided by the Court is subject to monitoring. Users of these services are therefore advised of this monitoring and agree to the practice. This monitoring may include a review of internet e:mail messages sent and received, and which Internet resources and sites are accessed.

- By participating in the use of the Internet systems provided by the Court, Users agree to be subject to and abide by the Court's Judicial and Clerk's Office Employee Internet Access Agreements. Willful violation of the general or specific provisions of the Internet Access Agreement Policy may result in disciplinary action, including termination.

- Intranet access is authorized to any federal court family WEB page or to the AO.

Virus Protection

A virus can be introduced into the Court System in a variety of ways:

- Software used at home but brought into the office by an employee may be infected and may infect office computers and/or the network.

- A program may be infected intentionally by a disgruntled employee, member of the computer user group or computer shareware organization.

- Viruses may be downloaded, directly or indirectly, from published bulletin boards.

- Viruses may also be introduced to computers from commercial software companies whose production facilities are infected.

There is no real, practical way to completely prevent computers from being attacked. To minimize exposure to viruses, follow the rules below:

- All new software, diskettes and files should be tested with a virus scanning program. Request help from the IT department if you need assistance with this process.

- Write-protect diskettes, especially original software distribution diskettes, and store them securely.

- Do not share diskettes unless they were previously scanned for viruses.

- Do not load programs from outside the Court or download programs from computer bulletin boards unless authorized by IT staff.

- Do not disable the virus scanning software that is installed on the computer system.

If a virus is introduced into the network or local computers, one or more of the following items may be noticed:

- Hard disk crashes,

- Files disappear,

- Files replicate unaccountably,

- Mystery file(s) appear,

- Data is changed or corrupted,

- Disk space mysteriously disappears,

- Memory capacity is reduced,

- Computer slows down or locks up, and

- Strange messages appear on the monitor.

Users can help identify the cause by:

- Staying calm,
- Discontinuing use of the computer,
- Writing down exactly what happened and what tasks you were performing, and
- Immediately calling the IT department to report the incident.

If a virus is located and removed, stay alert for reinfection.

Personal Computer Protection

Users must protect desktop computer equipment as follows:

- Protect equipment; keep food, drink and electrical appliances away from computers, diskettes and computer keyboard.
- Protect work areas; politely challenge anyone that is not recognized as belonging in the work area.

Electronic Mail

The policy regarding electronic mail (Lotus Notes) is as follows:

- Electronic mail from the Court's private data communication network is the property of the Court.
- Electronic mail from the Court's private data communication network should be primarily for official use; access to personal Internet web e-mail accounts is prohibited.
- Electronic mail may be monitored or accessed by management for various purposes (including backups).
- Before sending Electronic mail, staff should consider whether the message is essential or productive.

- Users are responsible for the maintenance of their e-mail. Due to a size limit of 450 MB, users should regularly clean up their in-boxes and sent mail folders by deleting messages or archiving.

- Electronic mail will not be used for the distribution of "chain letters."

- Electronic mail will not be used for the distribution of "jokes."

- Electronic mail will not utilized for the forwarding of non-business related messages with attachments from outside sources, including Executable files that have extensions (*.exe) and Image files (graphical), that have extensions (*.bmp, *.jpg, *.gif, *.tif).

If you have any doubts about the appropriateness of any electronic mail communication, seek the guidance of your supervisor or manager prior to transmission.

Screen Savers

Screen saver programs protect unauthorized access to data while users are away from their desks.

The policy for screen saver programs is as follows:

- Screen saver programs are required for all staff; they must not be turned off for any reason.

- The maximum activation time for screen savers will be no more than 10 minutes.

Automation Usage and Security Procedures

General Automation Policies

All judicial and clerk's office staff are required to comply with the general policies outlined below. Noncompliance with these policies may result in immediate disciplinary action which may include suspension or termination.

- Do not write or send abusive e-mail messages.
- Do not swear, use vulgarities or any other inappropriate language in electronic mail.
- Creation, transmission or publication of any obscene, indecent images, data or materials is prohibited.
- Using the network in such a way that would disrupt the use of the network by other users is prohibited.
- Any malicious attempt to harm or destroy data, hardware or software is prohibited.
- Browsing, exploring or making other unauthorized attempts to view data, files or directories belonging to other users is prohibited.
- Forging mail, attempting to use other users' accounts, attempting to crack password files, attempting to alter system files, and similar misbehavior is prohibited.
- Do not remove from the Court premises any computer equipment.
- Do not move or disconnect any computer equipment; contact the IT department for hardware relocation.
- No personal computer equipment shall be connected to the Court's network.
- Blogging in support of activities that are illegal, offensive or disparaging to fellow employees, the public or the judiciary, or that gives the impression of pronouncing official judicial policy is prohibited.

Automation Usage and Security Procedures

Acknowledgment of Receipt

1. I acknowledge that I have received and read the Automation Usage and Security Procedures for the United States District Court, Central District of California.

2. I acknowledge that it is my responsibility to conform to the standards and procedures outlined in this document.

3. I certify that I will abide by the policies outlined in this document.

4. I understand that non-compliance with the policies outlined in this document may result in disciplinary action which may include suspension or termination.

Printed Name	Signature
Title	Date
Judicial Chambers of Department	Telephone Number
Novell Login ID (not password)	CM/ECF Login ID (not password)
Supervisor's Name	