

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA  
OFFICE OF THE CLERK

---

MEMORANDUM

**FROM:** Jazmin Campos, Human Resources Specialist

**TO:** Judicial Assistants  
Incoming Externs

**SUBJECT:** Instructions Regarding Extern Paperwork/Background Check

This memo is intended to accompany each packet sent to incoming externs to assist them in completion of the required forms prior to starting their externship.

The forms included in this packet must be completed by the extern and returned to the Human Resources Department in advance of the start of the externship. This will allow for the required criminal background check to be completed prior to the extern's start date. Pursuant to the Court's security policy, externs will not be allowed to begin their duties until the criminal background check has been completed. Therefore, please return the completed documents as soon as possible.

The forms and individual instructions as to their completion are as follows:

- **Criminal Background Check Form** – This form needs to be completed by the extern as soon as possible before his or her start date. *It is imperative that a clear copy of the extern's driver's license is included.*
- **Fingerprint Card** – All externs must be fingerprinted in advance of their start date with the Court. Fingerprinting services are provided by law enforcement agencies as well as other businesses and can be easily located through an internet search. The completed fingerprint card should then be included with the rest of the materials returned to the Human Resources Department.
- **Current Address Form** – This form is completed by the extern.
- **Acknowledgment of Gratuitous Service and Waiver Under a Cooperative Educational Program (School Credit)** – This form is completed by the extern.
- **Computer Security Manual** – The extern completes the last page (receipt) but keeps the booklet. The job title is "Extern." Do not be concerned about the "log in" information, it will be added later but do include the judge's name.

- **Internet Access Agreement** – The extern completes the last page (receipt) but keeps the booklet. *Include the judge's name under "Department."*
- **Confidentiality Statement** – The extern must sign the back page and return it along with the other extern documents.
- **Employment Eligibility Verification (I-9)** – The extern is to complete section one only. **IMPORTANT:** The extern must bring one document from List A **OR** one document each from List B *and* List C. See reverse side of the form for the types of documents needed.

If you have any questions, please call Jazmin Campos at (213) 894-8505.

Enclosures

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

**EXTERN I.D. CARD APPLICATION/ BACKGROUND CHECK**

Name: \_\_\_\_\_

Current Address: \_\_\_\_\_  
\_\_\_\_\_

Telephone Number: \_\_\_\_\_

Social Security Card Number \_\_\_\_\_ (photo copy attached)

Driver's License Number \_\_\_\_\_ (photo copy attached)

Birth date: \_\_\_\_\_

Prior Names: \_\_\_\_\_

Externing for Judge: \_\_\_\_\_

Anticipated ending date: \_\_\_\_\_

Law School Extern Attending: \_\_\_\_\_

I agree to having a background investigation done prior to being issued an Identification Card (I.D.) by the U.S. District Court. I further agree to surrender any

I. D. card issued to me to the Clerk of Court at the end of my externship with the court.

Dated: \_\_\_\_\_

Signature

***Note: This form and photocopies of Social Security Card and Drivers license must be sent to Human Resources, 312 No. Spring Street, Room 535, Los Angeles, CA 90012, as soon as possible, but no later than two (2) months prior to your starting date with the judge.***

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**EMERGENCY CONTACT AND MEDICAL INFORMATION**  
PLEASE TYPE OR PRINT CLEARLY WHEN COMPLETING THIS INFORMATION

**CURRENT ADDRESS**

EMPLOYEE NAME		DATE OF BIRTH
STREET ADDRESS		APARTMENT NUMBER
CITY	STATE	ZIP CODE
HOME TELEPHONE	WORK TELEPHONE	EXTENSION OR DEPARTMENT
OPTIONAL: CELL PHONE NUMBER	OPTIONAL: PERSONAL E-MAIL ADDRESS(S) (TO BE USED IN AN EMERGENCY)	

LIST ANY MEDICAL INFORMATION (INCLUDING ALLERGIES OR DISABILITIES) WHICH MAY ASSIST US IN THE EVENT OF AN EMERGENCY:

\_\_\_\_\_

\_\_\_\_\_

**EMERGENCY CONTACT**

PLEASE MAKE SURE THAT THE PERSON TO BE NOTIFIED IN CASE OF AN EMERGENCY MAY BE REACHED DURING **REGULAR BUSINESS HOURS**. IF THE PERSON IS REGULARLY EMPLOYED, PLEASE PROVIDE A WORK TELEPHONE NUMBER AS WELL AS A HOME TELEPHONE NUMBER.

NAME		RELATIONSHIP
STREET ADDRESS		APARTMENT NUMBER
CITY	STATE	ZIP CODE
HOME TELEPHONE	WORK TELEPHONE	EXTENSION OR DEPARTMENT

**OUT OF STATE CONTACT**

NAME		RELATIONSHIP
STREET ADDRESS		APARTMENT NUMBER
CITY	STATE	ZIP CODE
HOME TELEPHONE	WORK TELEPHONE	EXTENSION OR DEPARTMENT

**PHYSICIAN INFORMATION**

NAME		TELEPHONE NUMBER
STREET ADDRESS		SUITE
CITY	STATE	ZIP CODE

\_\_\_\_\_

*Date Signed*

\_\_\_\_\_

*Signature of Employee*

Department of Homeland Security  
U.S. Citizenship and Immigration Services

**Form I-9, Employment Eligibility Verification**

Read instructions carefully before completing this form. The instructions must be available during completion of this form.

**ANTI-DISCRIMINATION NOTICE:** It is illegal to discriminate against work-authorized individuals. Employers CANNOT specify which document(s) they will accept from an employee. The refusal to hire an individual because the documents have a future expiration date may also constitute illegal discrimination.

**Section 1. Employee Information and Verification** (To be completed and signed by employee at the time employment begins.)

Print Name: Last		First	Middle Initial	Maiden Name
Address (Street Name and Number)			Apt. #	Date of Birth (month/day/year)
City	State	Zip Code	Social Security #	

I am aware that federal law provides for imprisonment and/or fines for false statements or use of false documents in connection with the completion of this form.

I attest, under penalty of perjury, that I am (check one of the following):

- A citizen of the United States
- A noncitizen national of the United States (see instructions)
- A lawful permanent resident (Alien #) \_\_\_\_\_
- An alien authorized to work (Alien # or Admission #) \_\_\_\_\_ until (expiration date, if applicable - month/day/year)

Employee's Signature	Date (month/day/year)
----------------------	-----------------------

**Preparer and/or Translator Certification** (To be completed and signed if Section 1 is prepared by a person other than the employee.) I attest, under penalty of perjury, that I have assisted in the completion of this form and that to the best of my knowledge the information is true and correct.

Preparer's/Translator's Signature	Print Name
Address (Street Name and Number, City, State, Zip Code)	Date (month/day/year)

**Section 2. Employer Review and Verification** (To be completed and signed by employer. Examine one document from List A OR examine one document from List B and one from List C, as listed on the reverse of this form, and record the title, number, and expiration date, if any, of the document(s).)

List A	OR	List B	AND	List C
Document title: _____	OR	_____	_____	_____
Issuing authority: _____		_____	_____	_____
Document #: _____		_____	_____	_____
Expiration Date (if any): _____		_____	_____	_____
Document #: _____		_____	_____	_____
Expiration Date (if any): _____	_____	_____	_____	_____

**CERTIFICATION:** I attest, under penalty of perjury, that I have examined the document(s) presented by the above-named employee, that the above-listed document(s) appear to be genuine and to relate to the employee named, that the employee began employment on (month/day/year) \_\_\_\_\_ and that to the best of my knowledge the employee is authorized to work in the United States. (State employment agencies may omit the date the employee began employment.)

Signature of Employer or Authorized Representative	Print Name	Title
Business or Organization Name and Address (Street Name and Number, City, State, Zip Code)		Date (month/day/year)

**Section 3. Updating and Reverification** (To be completed and signed by employer.)

A. New Name (if applicable)	B. Date of Rehire (month/day/year) (if applicable)
-----------------------------	--

C. If employee's previous grant of work authorization has expired, provide the information below for the document that establishes current employment authorization.

Document Title: \_\_\_\_\_ Document #: \_\_\_\_\_ Expiration Date (if any): \_\_\_\_\_

I attest, under penalty of perjury, that to the best of my knowledge, this employee is authorized to work in the United States, and if the employee presented document(s), the document(s) I have examined appear to be genuine and to relate to the individual.

Signature of Employer or Authorized Representative	Date (month/day/year)
--	-----------------------

## LISTS OF ACCEPTABLE DOCUMENTS

All documents must be unexpired

### LIST A

**Documents that Establish Both  
Identity and Employment  
Authorization**

### LIST B

**Documents that Establish  
Identity**

### LIST C

**Documents that Establish  
Employment Authorization**

	OR	AND
1. U.S. Passport or U.S. Passport Card	1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address	1. Social Security Account Number card other than one that specifies on the face that the issuance of the card does not authorize employment in the United States
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)		
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa	2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address	2. Certification of Birth Abroad issued by the Department of State (Form FS-545)
4. Employment Authorization Document that contains a photograph (Form I-766)	3. School ID card with a photograph	3. Certification of Report of Birth issued by the Department of State (Form DS-1350)
	4. Voter's registration card	
5. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form	5. U.S. Military card or draft record	4. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
	6. Military dependent's ID card	
	7. U.S. Coast Guard Merchant Mariner Card	5. Native American tribal document
	8. Native American tribal document	6. U.S. Citizen ID Card (Form I-197)
	9. Driver's license issued by a Canadian government authority	
<b>For persons under age 18 who are unable to present a document listed above:</b>		7. Identification Card for Use of Resident Citizen in the United States (Form I-179)
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI	10. School record or report card	8. Employment authorization document issued by the Department of Homeland Security
	11. Clinic, doctor, or hospital record	
	12. Day-care or nursery school record	

**Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)**

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**CONFIDENTIALITY STATEMENT**

One of the most important obligations of judicial employees is to ensure that nonpublic information learned in the course of employment is kept confidential. In the performance of job duties, employees may have access to files, records, draft materials, and conversations that are, under the Code of Conduct for Judicial Employees or by practice of the court, confidential. Canon 3D of the Code sets forth the minimum standard:

A judicial employee should avoid making public comment on the merits of a pending or impending action and should require similar restraint by personnel subject to the judicial employee's direction and control. This proscription does not extend to public statements made in the course of official duties or to the explanation of court procedures. A judicial employee should never disclose any confidential information received in the course of official duties except as required in the performance of such duties, nor should a judicial employee employ such information for personal gain. A former judicial employee should observe the same restrictions on disclosure of confidential information that apply to a current judicial employee, except as modified by the appointing authority.

**1. Confidential Information**

Confidential information means information received in the course of judicial duties that is not public and is not authorized to be made public. This includes information received by the court pursuant to a protective order or under seal; expressly marked or designated by a judge to be kept confidential; or relating to the deliberative processes of the court or an individual judge. Examples of confidential information are:

- (a) the substance of draft opinions or decisions;
- (b) internal memoranda, in draft or final form, prepared in connection with matters before the court;
- (c) the content or occurrence of conversations among judges or between a judge and judicial employees concerning matters before the court;
- (d) the identity of panel members or of the authoring judge before release of this information is authorized by the court;
- (e) the authorship of per curiam opinions or orders;
- (f) the timing of a decision, order, or other judicial action, including the status of or progress on a judicial action not yet finalized (except as authorized in accordance with Section 2.C.);
- (g) views expressed by a judge in the course of discussions about a particular matter before the court; and
- (h) any subject matter the appointing authority has indicated should not be revealed, such as internal office practices, informal court procedures, the content or occurrence of statements or conversations, and actions by a judge or staff.

Information that is not considered confidential includes court rules, published court procedures, public court records including the case docket, and information disclosed in public court documents or proceedings.

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**CONFIDENTIALITY STATEMENT**

**2. Nondisclosure**

**A. Unauthorized disclosure.** To promote public confidence in the integrity of the judicial system and to avoid impropriety, illegality, or favoritism, or any appearance thereof, it is critical that confidential information not be disclosed by a judicial employee. No past or present judicial employee may disclose or make available confidential information, except as authorized in accordance with Section 2.C.

**B. Inadvertent disclosure.** Sometimes breaches of confidentiality do not involve intentional disclosure but are the result of overheard remarks, casual comments, or inadequate shielding of sensitive materials. Judicial employees should take care to prevent inadvertent disclosure of confidential information by avoiding:

- (1) case-related conversations and other discussions of confidential information in public places within the court, such as the library, hallways, elevators, and cafeteria;
- (2) case-related conversations and other discussions of confidential information at bar association meetings, law schools, other gatherings of noncourt persons, or in public places;
- (3) exposure of confidential documents to the view of noncourt persons;
- (4) visible display of confidential documents in public places such as a library, on public transportation, or in a photocopier or scanner to which noncourt persons have access;
- (5) substantive discussions with counsel, litigants, or reporters about the merits of a matter before the court;
- (6) use of writing samples from judicial employment without adequate redaction and approval of the appointing authority; and
- (7) internet and other electronic exchanges (anonymously, pseudonymously, or otherwise) about the court or its cases.

**C. Authorized disclosure.** Confidential information is authorized to be disclosed in the following circumstances:

- (1) pursuant to a statute, rule, or order of the court, or authorization from the appointing authority;
- (2) pursuant to a valid subpoena issued by a court or other competent body; and
- (3) to report an alleged criminal violation to the appointing authority or other appropriate government or law enforcement official.

**D. Continuing obligation.** Confidentiality obligations do not end when judicial employment ceases or when a matter is completed or a case is closed. Former judicial employees should observe the same restrictions on disclosure of confidential information that apply to current employees, except as modified in accordance with Section 2.C. Confidentiality restrictions continue to apply with respect to open as well as closed and completed matters.

**3. Acknowledgment**

To emphasize the importance of the duty of confidentiality, the court asks that you sign this statement as an acknowledgment that you have read it, understand it, and agree to abide by it, and further that you understand violations of these confidentiality obligations may result in disciplinary action.

---

*Signature*

---

*Date*

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**ACKNOWLEDGMENT OF GRATUITOUS SERVICES AND WAIVER UNDER A  
COOPERATIVE EDUCATIONAL PROGRAM**

---

I, \_\_\_\_\_, hereby declare that I will perform from approximately \_\_\_\_\_ to \_\_\_\_\_ for the United States District Court in connection with my participation in a cooperative educational program with \_\_\_\_\_. I further understand that the United States District Court is acting solely as a host in this arrangement by providing a work-related educational experience. I hereby waive any claim or right to receive salary or other compensation, including fringe benefits, from the Government as a result of my work/training services to \_\_\_\_\_, except that in the event of any personal injury incurred by me, I shall have those rights to compensation, if any, which may be provided by statute to persons rendering voluntary services to the United States. I further waive all right to any personal copyright privileges in any work product prepared by me in the course of my services to \_\_\_\_\_. Finally, I recognize that information which I shall have access to in the course of my educational experience is often of a confidential nature, and I agree to preserve the confidentiality of such information.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Witness

\_\_\_\_\_  
Date

Pursuant to the authority vested in the Director of the Administrative Office of the United States Courts by 28 U.S.C. § 604 (a) (17), and by delegation of this authority from the Director, I hereby accept and authorize the utilization of the gratuitous services described above.

\_\_\_\_\_  
Clerk of Court  
on behalf of the Director,  
Administrative Office of the  
United States Courts

Date: \_\_\_\_\_

**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 must not 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 be 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

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**



**JUDICIAL EMPLOYEE (EXTERN / INTERN)  
INTERNET ACCESS AGREEMENT**

## JUDICIAL EMPLOYEE (EXTERN / INTERN) - INTERNET ACCESS AGREEMENT

---

### General Provisions

In compliance with Judicial Conference Policy regarding Internet access for computers connected to the Data Communications Network (DCN), the following general and specific provisions apply to all judicial employees including Externs and Interns, of the Central District of California:

1. Use of the public Internet network accessed via computer gateways owned or operated on the behalf of the United States District Court for the Central District of California ("the Court"), imposes certain responsibilities and obligations on Court employees and officials ("Users"), and is subject to Court policies and local, state and federal laws. Acceptable use is ethical, reflects honesty, and shows restraint in the consumption of shared computing resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and an individual's right to freedom from harassment and unwarranted annoyance.
2. 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 this practice. This monitoring may include a review of internet e-mail messages sent and received, and which Internet resources and sites are accessed. Users should further be advised that many external Internet sites also log who accesses their resources, and may make this information available to third parties.
3. By participating in the use of the Internet systems provided by the Court, Users agree to be subject to and abide by this Policy for their use. Willful violation of the general or specific provisions of the Policy may result in disciplinary action, including termination.

## JUDICIAL EMPLOYEE (EXTERN / INTERN) - INTERNET ACCESS AGREEMENT

---

### Specific Provisions

1. Users will not utilize the Internet network for illegal, unlawful, or unethical purposes or to support or assist such purposes. Examples of this would be the transmission (including uploading or downloading files) or viewing of violent, threatening, defrauding, obscene, or unlawful materials. Unless case-related, creating, downloading, viewing, storing, copying, and transmitting sexually-explicit or sexually-oriented materials is never appropriate and may be illegal in some cases.
2. Users will not utilize the Internet network equipment for partisan political purposes or commercial gain.
3. Unless for official business, judiciary employees, including Externs and Inters, should not use the network connection for commercial purposes (including shopping). It is also inappropriate to use the network connection in support of outside employment activities (including consulting for pay, sales or administration of business transactions, and sales of goods or services) or for illegal activities (such as gambling or hacking).
4. Users will not utilize the Internet systems or messaging services to harass, intimidate or otherwise annoy other persons.
5. It is not appropriate to use government systems to send or receive e-mails containing greeting cards, political statements, jokes, pictures, sexually-explicit or sexually-oriented materials and other items of a personal nature. Chain letters or other unauthorized mass mailings, regardless of the subject matter, likewise are inappropriate. Checking personal web e-mail accounts from the Court's private data communications network raises severe security risks locally and judiciary-wide and is prohibited.

6. Users will not utilize the Internet to disrupt other users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses, and sustained high volume network traffic which substantially hinders others in their use of the network. Logging onto video or audio sites, such as broadcast services or radio stations, degrades the performance of the entire network and is prohibited. Downloading music files consumes significant disk space on local computers and may be a violation of copyright law.
7. Users will only utilize the Internet network to access files and data that are their own, that are publicly available, or to which they have authorized access.
8. Because files or matters obtained over the Internet may contain destructive computer viruses that may be harmful to the Court's network, downloading attachments to e-mail or files obtained via the Internet (as opposed from the Intranet or DCN) shall be strictly limited to either: (1) items expressly requested by the Users from known senders, or (2) unrequested files transmitted to Users by known senders. Users shall not download and open any attachments to files, or open any e-mail, that is received or made available to the Users from an unknown Internet source.
9. Users will not remove Court scanning software. If the software is removed or not activated and use of the Internet has been or is being performed, the Users may lose their right to access the Internet and the DCN.
10. Users will refrain from monopolizing systems, overloading networks with excessive data, or otherwise disrupting the network systems for use by others. Video, sound or other large file attachments consume large amounts of network capacity. E-mail attachments, large files, and executable programs present two problems: first,

large attachments consume network capacity and storage space on both national and local e-mail servers and desktops, slowing down the network for everyone; and second, executable programs present a risk for infection by computer viruses.

11. Judiciary employees, including Externs and Interns, should only participate in chat rooms when directly relevant to their official duties and responsibilities. All other non-business related chat rooms are prohibited. When participating in a chat room, Users should not inadvertently give the impression of articulating official judiciary policy or positions. The use of peer-to-peer file sharing, chat rooms, and instant messaging for communicating with persons or entities outside the judiciary's private data communications network is prohibited.
12. It is not appropriate to use e-mail or the Internet to access, send or receive information on or in support of activities that are illegal or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
13. 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.

**JUDICIAL EMPLOYEE (EXTERN / INTERN) - INTERNET ACCESS AGREEMENT**

---

By signing this Agreement, I agree to abide by the general and specific provisions outlined and understand that use of the public Internet is a privilege that can be revoked if improperly used.

\_\_\_\_\_  
*Dated*

\_\_\_\_\_  
*Employee Signature*

\_\_\_\_\_  
*Print Name*

\_\_\_\_\_  
*Chambers*