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

MEMORANDUM

FROM: **Lisa Lyons**, Human Resources Assistant

TO: Incoming Interns

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

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

The forms included in this packet must be completed by the intern and returned to the Human Resources Department in advance of the start of the internship. This will allow for the required criminal background check to be completed prior to the intern's start date. Pursuant to the Court's security policy, interns will not be allowed to begin their duties or receive an identification badge until the criminal background check has been completed. It takes on average approximately 2-3 weeks for a background check to be completed. Therefore, **please return the completed documents as soon as possible.**

The forms with instructions are listed below:

- **Criminal Background Check Form** – This form needs to be completed by the intern as soon as possible before his or her start date. *It is imperative that a clear copy of two forms of identification are included.* Examples of acceptable forms of identification include a Driver's License, Social Security card, an unexpired U.S. Passport and Birth Certificate.

- **Fingerprint Card** – All interns 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 ***as soon as possible***. Please do not wait until your first day to submit the fingerprint card as this will delay the clearance from being received in a timely manner. **Identification cards WILL NOT be issued without background clearance.**

- **Current Address Form** – This form is completed by the intern.

- **Acknowledgment of Gratuitous Service and Waiver** – This form is completed by the intern.

- **Computer Security Manual** – The intern completes the last page (receipt) but keeps the booklet. The job title is what ever department and "Intern." Do not be concerned about including phone numbers or log in information, but do include the manager's name.

- **Internet Access Agreement** – The intern completes the last page (receipt) but keeps the booklet.

- **Confidentiality Statement** – The intern must sign the back page and return it along with the other intern documents.

- **Employment Eligibility Verification (I-9)** – The intern is to complete section one only. **IMPORTANT:** The intern must provide 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.

- **Social Media Privacy Tips & Social Media and Social Networking Policy** – Memorandum and Court policy on the use of social media.

- **United States Court Appointment** – The intern must fill out his/her full legal name, date of entrance on duty (start date), duty station (city where internship will take place), legal name in section B and sign as the appointee. The oath will be administered either in chambers or in the Human Resources office prior to commencing the assignment.

All completed documents, including the completed fingerprint card, must be returned to the Human Resources office. The address is:

U.S. District Court
Human Resources
312 N. Spring St, Room 535
Los Angeles, CA 90012

If you have any questions, please call Lisa Lyons at (213) 894-6366.

Enclosures

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

INTERN 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: _____

Department: _____

Anticipated ending date: _____

School Intern 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 internship 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.

CLEAR FORM

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

AO 196A
(Rev. 11/10)

ACKNOWLEDGMENT OF GRATUITOUS SERVICES AND WAIVER

I, _____ , hereby declare that my services to be performed from approximately _____ to _____ in the capacity of _____ to _____ in the United States _____ *(court or office)* are to be solely as a volunteer. I hereby waive any claim or right to receive salary or other compensation in consideration for the performance of duties assigned by _____ . I acknowledge that I am not entitled to receive civil service retirement credit or other related personnel benefits as a consequence of this voluntary employment, 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 recognize that, as an employee of the United States, I retain no personal copyright privileges in any work product prepared by me in the course of this employment. Finally, I recognize that information which I obtain or to which I shall have access in the course of my employment 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.

_____ _____

Signature of the Court Unit Executive Date

Print Save As... Reset

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 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

CLERK'S OFFICE EMPLOYEE

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 clerk's office employees 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.

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. 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 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 the network down for everyone; and second, executable programs

present a risk for infection by computer viruses.

11. Judiciary employees 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, employees 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.

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

Department

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*

OMB No. 1615-0047; Expires 08/31/12

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:				
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**	OR	LIST B **Documents that Establish Identity**	AND	LIST C **Documents that Establish Employment Authorization**
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)				**2.** Certification of Birth Abroad issued by the Department of State (Form FS-545)
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		**3.** Certification of Report of Birth issued by the Department of State (Form DS-1350)
4. Employment Authorization Document that contains a photograph (Form I-766)		**3.** School ID card with a photograph		
		4. Voter's registration card		**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
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		
		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		
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		**For persons under age 18 who are unable to present a document listed above:**		**7.** Identification Card for Use of Resident Citizen in the United States (Form I-179)
		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)

SOCIAL MEDIA PRIVACY TIPS
How to Protect Your Privacy on the Internet

Social media, professional networking sites, rapid-fire communications, blog sites, and personal web sites are all widespread, relatively new communications technologies. However, the rules for maintaining your safety and privacy with respect to social media sites on the Internet are identical or similar to the rules for other communication methods, such as writing, telephone and even oral or written conversation.

Social networking sites on the Internet now include (but are not limited to):

Classmates	MySpace
Digg	Personal Blogs
Facebook	Personal Web Sites
Flickr	Twitter
LinkedIn	Yahoo! Groups
LiveJournal	YouTube

In order to maximize privacy and safety, make sure your home PC's and laptops have an enabled firewall installed and anti-virus software that regularly updates its virus signatures to protest you from outside virus threats. (The Court allows Court employees to install Symantec Anti-Virus Corporate Edition on their personal computers to help prevent the spread of viral threats to court computer systems through shared media.)

Social media sites prompt you for a lot of personal information when you set up an account. You should avoid providing personal information that anyone could ultimately use for nefarious purposes. This would include your social security number, home address, phone number, names for family members, and the name and address of your employer.

Do not use your court email address or your regular personal email address as your contact name for any online social networking application. Create and use separate email accounts from either your Internet service provider or from free email services, such as Hotmail or Gmail, to use as a contact address of as a user id for social networking sites.

On any social networking site, limit the access your networking friends, their friends, and the Internet world as a whole, have to the content of the information you post on the site. Do not permit the world to have access to the same information as you would your family or close personal friends. For example, you may want to restrict your phone number to be available to select networking friends and family.

Be careful with images and pictures you post on social networking sites or send to friends via an email. Whether intended or not, **anything** you publish on the Internet becomes essentially part of the public domain. Be aware also that anything you publish on the Internet may be used in illegal or unethical ways.

While you may be able to control what you post, you can neither control nor predict what others, even family and friends, might post on your page or in a blog. Their actions, while harmless in intent, could ultimately embarrass you or the Court, or even place you in danger.

Be mindful of what you click on within a social networking site, an email, or a chat site (instant messaging). Even well-established sites have been known to inadvertently allow a dubious link to be accessed by its members, thus allowing malicious software to be installed on the member's PC. If an unsolicited invitation comes along touting information or offers that sound to good to be true, steer clear of these sites. Do not click on any links except for the Close button located in the top right-hand corner of the window.

Regular screen the social media sites in which you participate to ensure that nothing is posted that goes against your best wishes and intent. Should such items appear, it is your responsibility to report such defamation to the administrators of the social networking or web site, to immediately delete the communication, and to consider shutting down your social network site or account altogether.

UNITE D STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SOCIAL MEDIA AND SOCIAL NETWORKING POLICY AND ACKNOWLEDGMENT OF RECEIPT CLERK'S OFFICE EMPLOYEE

April 1, 2010

1. AUTHORITY

This social media and social networking policy applies to all Clerk's Office employees of the United States District Court, Central District of California, including those employees under its supervision or administration, such as capital habeas staff attorneys, pro se staff attorneys, and court reporters (collectively referred to as the *employees*). This policy should be read in conjunction with the Code of Conduct for Judicial Employees, the Court's Employee Manual, the Clerk's Office Employee Internet Access Agreement, and the Court's Job Behavior and Conduct Expectations policy (Chapter 3, § 3.07 of the Employee Manual).

This policy is approved and administered by the Clerk of Court. The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exist, employees should use good judgment and take the most prudent action possible. Employees should consult with their manager or supervisor if uncertain.

2. USE OF SOCIAL MEDIA

Social media, professional networking sites, rapid-fire communications, blog sites, and personal web sites are all widespread, relatively new, communication technologies. The rules for use of this social media with respect to Court employment, however, are identical to the rules for use of other communication methods (such as writing or publishing, telephoning, or even conversation).

Many users of social media identify their employer or occupation. An employee clearly identifies association with the Court by using the employee's court email address to engage in social media or professional social networking activity. As stated in Section 6, the use of the employee's court email address to engage in social media or professional social networking activity is prohibited.

Employees must use good judgement and careful discretion about the material or information posted online.

3. PRINCIPLES

The Court's reputation for impartiality and objectivity is crucial. The public must be able to trust the integrity of the Court. The public needs to be confident that the outside activities of our

employees do not undermine the Court's impartiality or reputation and that the manner in which the Court's business is conducted is not influenced by any commercial, political, or personal interests. Do not identify yourself as a Court employee. By identifying oneself as an employee of the United States District Court, a social networker becomes, to some extent, a representative of the Court, and everything he/she posts has the potential to reflect upon the Court and its image. It is acknowledged that without identifying oneself as a Court employee, an employee may intentionally or unintentionally reveal information that will allow the inference of Court employment. If this occurs, the employee assumes the responsibility for representing the Court in a professional manner.

4. RESPONSIBILITY

Any material, including photographs, presented online on a Court employee website, social media, or email or blog, that pertains to the Court by any poster is the responsibility of the Court employee, even if Court employment can only be indirectly inferred or deduced. Personal blogs should not identify Court employment even indirectly; if possible, use your first name only. Do not reference or cite other Court employees without their express consent, and even then, do not identify them as Court employees.

5. RELEVANT TECHNOLOGIES

This policy includes (but is not limited to) the following specific technologies:

- Classmates
- Digg
- Facebook
- Flickr
- LinkedIn
- LiveJournal
- MySpace
- Personal Blogs
- Personal Websites
- Twitter
- Yahoo! Groups
- YouTube

6. RULES

- Use of the court email address for social networking (for example, blogs, Facebook, Twitter) is not permitted. Use of an employee's court email address is subject to the same appropriate use policies pertaining to the use of the telephone, namely, limited personal use not interfering with the performance of work responsibilities. Email addresses should not be used for "chain" correspondence, solicitation of donations, transmittal of large audio, video or other large files, or any business enterprise.

- The Court policy is not to identify yourself as a court employee at all in social media. While you can control what you post, you cannot predict nor control what others, even family members or friends, might post on your page or in a blog. Their actions, while harmless in intent, could end up embarrassing you, the Court, or worse yet, put you in some danger.

- Maintain professionalism, honesty, and respect. Consider your online dialogue as subject to the same bounds of civility required at work. Employees must comply with laws covering libel and defamation of character. Even non-Court specific behavior could have ramifications on your employment status (e.g. photographs in compromising or illegal situations).

- Do not discuss your job responsibilities for the Court on the Internet. Be careful to avoid leaking confidential information. Avoid negative commentary regarding the Court. Any commentary you post that could reveal an association with the Court must contain an explicit disclaimer that states: "These are my personal views and not those of my employer." Again, remember that even harmless remarks could be misconstrued by litigants unfamiliar with court processes (such as pro se litigants).

- Observe security protocol. Employees must take care to avoid doing things that would compromise the security of the courthouse and personnel. To maintain security do not post pictures of the courthouse, inside or outside; do not post pictures of court events; and do not post pictures of the Court's judicial officers.

- Regularly screen the social media or websites that you participate in to ensure nothing is posted which is contrary to the best interests of the Court. Should such items appear, it is your responsibility to contact your supervisor and then immediately delete the communication or information, even closing down your Facebook page, etc., as necessary.

- Further, if any employee becomes aware of social networking activity of other staff that would be deemed distasteful or fail the good judgment test, please contact your supervisor.

7. PRODUCTIVITY IMPACT

The use of Court assets (computers, Internet access, email, etc.) is intended for purposes relevant to the responsibilities assigned to each employee. Social networking sites are not deemed a requirement for any position, and certain job titles are not permitted to access these services at work. For employees that are allowed to access these services, social media activities should not interfere with work commitments, and must comply with the signed Internet Access Agreement. Unless otherwise authorized by the Judge, employees who work in the courtroom are prohibited from using computers, handheld wireless devices, blue-tooth enabled earpieces and headsets, and other hands-free wireless devices, for non-work related reasons when court is in session or the courtroom is otherwise occupied.

8. COPYRIGHT

Employees must comply with all copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.

9. TERMS OF SERVICE

Most social networking sites require that users, when they sign up, agree to abide by a Terms of Service document. Court employees are responsible for reading, knowing, and complying with the terms of service of the sites they use. It is not the policy of the Court to require employees to use pseudonyms when signing up for social networking sites; however, for some employees in sensitive positions, this might be wise. Employees should check the Information Technology Department regarding any questions about Terms of Service agreements when accessing the Internet at work.

10. OFF LIMITS MATERIAL

This policy sets forth the following items which are deemed off-limits for social networking whether used at Court or after work on personal computers, irrespective of whether Court employment is identified:

Seal and Logos

The United States District Court seal and logos may not be used in any manner.

Politically Sensitive Areas

Employees may not be seen to support any political party or cause. Employees should never indicate a political allegiance on social networking sites, either through profile information or through joining political groups. Employees should not express views for or against any policy which is a matter of current party political debate. Employees should not advocate any particular position on an issue of current public controversy or debate. If an employee is in doubt, they should refer immediately to their supervisor or manager.

The Hatch Act, 5 U.S.C. § 7324 et seq., regulates the participation of government employees, as defined in 5 U.S.C. § 7322(1), in certain types of partisan political activities. Although the Hatch Act is not applicable to the Judicial Branch, the Judicial Conference has adopted similar restrictions. Canon 5 of the Code of Conduct for Judicial Employees prohibits all active engagement in partisan political activities, including, but not limited to, public endorsement of a candidate or contribution to a political campaign. The Code of Conduct should be consulted for a thorough understanding of the specific prohibitions on political activity contained in Canon 5. In addition, Advisory Opinion No. 92 provides guidelines for political activities.

Confidential Information

One of the most important obligations of employees is to ensure that non-public information learned in the course of employment is kept confidential. Confidential information is strictly forbidden from any discourse outside of the appropriate employees of the Court. Information published on blog(s) must comply with the Court's confidentiality policies. This also applies to comments posted on other blogs, forums, and social networking sites. Confidential information is not to be discussed or referred to on such sites, even in private messages between site members who have authorized access to the information. Court employees should also refrain from discussing any of the Court's internal processes and procedures, whether they are of a non-confidential or confidential nature.

Online Recommendations

Some sites, such as LinkedIn, allow members to "recommend" current or former co-workers. If an employee does this as a representative of the Court, it may give the appearance that the Court endorses the individual being recommended. This could create a liability situation if another entity hires the recommended person on the basis of the recommendation. Accordingly, the Court forbids employees to participate in employee recommendations for reasons of liability. All communication of this type should be referred to Human Resources for verification.

11. MONITORING EMPLOYEES' USE OF SOCIAL MEDIA

The Court reserves the right to monitor its employees' use of Social Media by monitoring its employees' Internet activities as set forth in the Clerk's Office Employee Internet Access Agreement. The Court further reserves the right to visit and monitor Social Media sites to ensure that employees are not violating our Court's Social Media Policy via Court or any other computers, including employees' own personal computers.

12. DISCIPLINARY ACTION

Employees who participate in online communication deemed not to be in the best interest of the Court may be subject to disciplinary action. Inappropriate communication can include, but is not limited to:

Confidential Court information or data leakage.
Inaccurate, distasteful, or defamatory commentary about the Court.
Behavior or communication encouraging behavior that is illegal, grossly unprofessional or in bad taste.

Disciplinary action can include termination or other intervention deemed appropriate by Human Resources. Please refer to the Employee Manual for information on the appeal procedures for disciplinary actions.

13. COURT REPORTER EXCEPTION

Official court reporters have an authorized business reason to establish and maintain websites that identify the Court as their place of employment.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SOCIAL MEDIA AND SOCIAL NETWORKING POLICY AND ACKNOWLEDGMENT OF RECEIPT CLERK'S OFFICE EMPLOYEE

1. I acknowledge that I have received and read the Clerk's Office Employee Social Media and Social Networking Policy 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
Department	Telephone Number

✎AO 78A (11/06)

United States Courts Appointment

A

Judge's Staff:

_____ Yes ☐ No ☑

(Name of Court)

_____ is appointed.

(Name as it is signed below)

INTERN _____ _____

(Position title) (Date of entrance on duty) (Duty station)

(Vice _____ ; Sep _____

(Previous incumbent) mo. day yr.

Clerk of Court _____

(Title of appointing officer) (Signature of appointing officer)

(Note: Appointing officer, please indicate the grade or level recommended N/A) Special pay rate? Yes ☐ No ☐

B

I, _____ , do solemnly swear (or affirm) that

A. OATH OF OFFICE

I will support and defend the constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

D. AFFIDAVIT AS TO EMOLUMENT FROM FOREIGN OFFICE

I will not accept, nor am I accepting any present emolument, office or title, of any kind whatever, from any King, Prince, or foreign state.

E. AFFIDAVIT AS TO PERSONAL HISTORY AND EXPERIENCE AND QUALIFICATIONS STATEMENTS

The information given concerning personal history, experience and qualifications is true and correct to the best of my knowledge and belief.

_____

(Signature of appointee)
(Name will be on records as signed)

Subscribed and sworn (or affirmed) before me this _____ day of _____ 20 _____

at LOS ANGELES , CALIFORNIA

(City) (State)

_____

(Signature of officer)

_____

(Title)

(SEAL)

(Note: The words "So help me God" in the oath and the word "swear" wherever it appears above should be stricken out when the appointee elects to affirm rather than swear to the affidavits; only these words may be stricken and only when the appointee elects to affirm the affidavits.

APPOINTMENT IS NOT COMPLETE UNTIL OATH OF OFFICE IS ADMINISTERED.

FINGERPRINT CARD INSTRUCTIONS

Fingerprint Card -All extems must be fingerprinted **in advance** of their start date with the court. The fingerprint form must be taken to a law enforcement agency or place of business so the fingerprints can be completed. The extern is to complete all areas at the top of the form with their personal information. The box marked (MNU) is for placement of the Driver's License or Identification Card number. The form is then included with the rest of the materials that are returned to the Human Resources office.

COURT ADDRESS

U.S. District Court
Human Resources
312 N. Spring St, Room 535
Los Angeles, CA 90012

APPLICANT
* See Privacy Act Notice on Back

FD-258 (REV.12-10-07)

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM | FIRST NAME | MIDDLE NAME

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED

ALIASES AKA

ORI

RESIDENCE OF PERSON FINGERPRINTED

DATE OF BIRTH DOB
Month Day Year

CITIZENSHIP CTZ

SEX | RACE | HGT. | WGT. | EYES | HAIR

PLACE OF BIRTH POB

DATE | SIGNATURE OF OFFICIAL TAKING FINGERPRINTS

YOUR NO. OCA

EMPLOYER AND ADDRESS

FBI NO. FBI

LEAVE BLANK

CLASS

ARMED FORCES NO. MNU

REF.

REASON FINGERPRINTED

SOCIAL SECURITY NO. SOC

MISCELLANEOUS NO. MNU

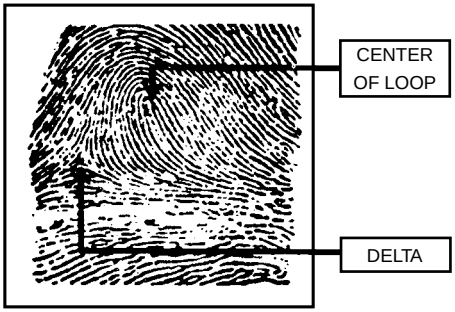
1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING	5. R. LITTLE
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING	10. L. LITTLE

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY | L. THUMB | R. THUMB | RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
CJIS DIVISION/CLARKSBURG, WV 26306

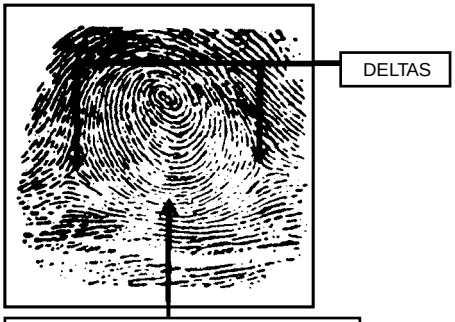
APPLICANT

1. LOOP



THE LINES BETWEEN CENTER OF LOOP AND DELTA MUST SHOW

2. WHORL



THESE LINES RUNNING BETWEEN DELTAS MUST BE CLEAR

3. ARCH

ARCHES HAVE NO DELTAS

FD-258 (REV. 12-10-07)

THIS CARD FOR USE BY:

1. LAW ENFORCEMENT AGENCIES IN FINGERPRINTING APPLICANTS FOR LAW ENFORCEMENT POSITIONS.*
2. OFFICIALS OF STATE AND LOCAL GOVERNMENTS FOR PURPOSES OF EMPLOYMENT, LICENSING, AND PERMITS, AS AUTHORIZED BY STATE STATUTES AND APPROVED BY THE ATTORNEY GENERAL OF THE UNITED STSTES. LOCAL AND COUNTY ORDINANCES, UNLESS SPECIFICALLY BASED ON APPLICABLE STATE STATUTES DO NOT SATISFY THIS REQUIREMENT.*
3. U.S. GOVERNMENT AGENCIES AND OTHER ENTITIES REQUIRED BY FEDERAL LAW.**
4. OFFICIALS OF FEDERALLY CHARTERED OR INSURED BANKING INSTITUTIONS TO PROMOTE OR MAINTAIN THE SECURITY OF THOSE INSTITUTIONS.

Please review this helpful information to aid in the successful processing of hard copy criminal and civil fingerprint submissions in order to prevent delays or rejections. Hard copy fingerprint submissions must meet specific criteria for processing by the Federal Bureau of Investigation.

Ensure all information is typed or legibly printed using blue or black ink.
Enter data within the boundaries of the designated field or block.
Complete all required fields. (If a required field is left blank, the fingerprint card may be immediately rejected without further processing.)

- The required fields for hard copy fingerprint cards are: originating agency identifier number - date of birth - place of birth - name - sex fingerprint impressions - any applicable state stamp - Other (race, height, weight, eye color, hair color)
  * criminal fingerprint cards also require an arrest charge and date of arrest.
  * civil fingerprint cards also require a reason fingerprinted and date fingerprinted

Do not use highlighters on fingerprint cards.
Do not enter data or labels within 'Leave Blank' areas.
Ensure the 'Reply Desired' field is checked when applicable (criminal only**).**
Ensure fingerprint impressions are rolled completely from nail to nail.
Ensure fingerprint impressions are in the correct sequence.
Ensure notations are made for any missing fingerprint impression (i.e. amputation).
Do not use more than two retabs per fingerprint impression block.
Ensure no stray marks are within the fingerprint impression blocks.

Training aids can be ordered online via the Internet by accessing the FBI's website at: fbi.gov, click on 'Fingerprints', then click on 'Ordering Fingerprint Cards & Training Aids'. Direct questions to the Identification and Investigative Services Section's Customer Service Group at (304) 625-5590 or by e-mail at <liaison@leo.gov>.

PRIVACY ACT STATEMENT

Authority: The FBI's acquisition, preservation, and exchange of information requested by this form is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include numerous Federal statutes, hundreds of State statutes pursuant to Pub.L. 92-544, Presidential executive orders, regulations and/or orders of the Attorney General of the United States, or other authorized authorities. Examples include, but are not limited to: 5 U.S.C. 9101; Pub.L. 94-29; Pub.L. 101-604; and Executive Orders 10450 and 12968. Providing the requested information is voluntary; however, failure to furnish the information may affect timely completion or approval of your application.

Social Security Account Number (SSAN). Your SSAN is needed to keep records accurate because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 USC 552a), the requesting agency is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other authority your SSAN is solicited, and what uses will be made of it. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

Principal Purpose: Certain determinations, such as employment, security, licensing, and adoption, may be predicated on fingerprint-based checks. Your fingerprints and other information contained on (and along with) this form may be submitted to the requesting agency, the agency conducting the application investigation, and/or FBI for the purpose of comparing the submitted information to available records in order to identify other information that may be pertinent to the application. During the processing of this application, and for as long hereafter as may be relevant to the activity for which this application is being submitted, the FBI may disclose any potentially pertinent information to the requesting agency and/or to the agency conducting the investigation. The FBI may also retain the submitted information in the FBI's permanent collection of fingerprints and related information, where it will be subject to comparisons against other submissions received by the FBI. Depending on the nature of your application, the requesting agency and/or the agency conducting the application investigation may also retain the fingerprints and other submitted information for other authorized purposes of such agency(ies).

Routine Uses: The fingerprints and information reported on this form may be disclosed pursuant to your consent, and may also be disclosed by the FBI without your consent as permitted by the Federal Privacy Act of 1974 (5 USC 552a(b)) and all applicable routine uses as may be published at any time in the Federal Register, including the routine uses for the FBI Fingerprint Identification Records System (Justice/FBI-009) and the FBI's Blanket Routine Uses (Justice/FBI-BRU). Routine uses include, but are not limited to, disclosures to: appropriate governmental authorities responsible for civil or criminal law enforcement, counterintelligence, national security or public safety matters to which the information may be relevant; to State and local governmental agencies and nongovernmental entities for application processing as authorized by Federal and State legislation, executive order, or regulation, including employment, security, licensing, and adoption checks; and as otherwise authorized by law, treaty, executive order, regulation, or other lawful authority. If other agencies are involved in processing this application, they may have additional routine uses.

Additional Information: The requesting agency and/or the agency conducting the application-investigation will provide you additional information pertinent to the specific circumstances of this application, which may include identification of other authorities, purposes, uses, and consequences of not providing requested information. In addition, any such agency in the Federal Executive Branch has also published notice in the Federal Register describing any system(s) of records in which that agency may also maintain your records, including the authorities, purposes, and routine uses for the system(s).

INSTRUCTIONS:

* 1. PRINTS MUST GENERALLY BE CHECKED THROUGH THE APPROPRIATE STATE IDENTIFICATION BUREAU, AND ONLY THOSE FINGERPRINTS FOR WHICH NO DISQUALIFYING RECORD HAS BEEN FOUND LOCALLY SHOULD BE SUBMITTED FOR FBI SEARCH.

2. IDENTITY OF PRIVATE CONTRACTORS SHOULD BE SHOWN IN SPACE "EMPLOYER AND ADDRESS". THE CONTRIBUTOR IS THE NAME OF THE AGENCY SUBMITTING THE FINGERPRINT CARD TO THE FBI.

3. FBI NUMBER, IF KNOWN, SHOULD ALWAYS BE FURNISHED IN THE APPROPRIATE SPACE.

** MISCELLANEOUS NO. - RECORD: OTHER ARMED FORCES NO. PASSPORT NO. [FP], ALIEN REGISTRATION NO. (AR), PORT SECURITY CARD NO. (PS), SELECTIVE SERVICE NO. (SS) VETERANS' ADMINISTRATION CLAIM NO. (VA).