Print

UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

Welcome to the United States District Court for the District of New Jersey. This new intern appointment package complies with the Guide to Judiciary Policy on interns/externs/volunteers and contains important forms that must be completed prior to your first day of internship with the Federal Judiciary.

All of the forms must be completed and submitted electronically as a PDF document to the address listed below. All of the attached forms are in **PDF** fillable format, and use the latest Adobe Reader. If you do not have the latest Adobe Reader, you can install it by going to https://get.adobe.com/reader/. Please follow the instructions for each form in the package to ensure successful completion and review each form for accuracy prior to sending to the Human Resources Department for processing.

Interns/externs/volunteers should schedule a fingerprint appointment **at least 30 days prior to the start of internship**. Please contact the following individuals to schedule fingerprinting:

For Newark assigned interns:

Contact: David Rodriguez, HR Assistant at (973) 776-3879.
Fingerprint Location: Martin Luther King Federal Building and U.S. Courthouse
50 Walnut Street; 4th Floor Clerk's Office, Newark, NJ 07101

For Camden and Trenton assigned interns:

Contact: Brian Kemner, Emergency Preparedness Specialist at (609) 989-2333.
Fingerprint location: Camden
Mitchell H. Cohen Federal Building & U.S. Courthouse
4th and Cooper Streets, 1st floor, Camden, NJ 08101

FingerPrint Location: Trenton
Clarkson S. Fisher Federal Building and U.S. Courthouse
402 East State Street; 3rd Floor, Trenton, NJ 08608

Completed and signed forms along with copies of requested valid Driver's License, U.S. Passport and/or Social Security card must be returned as a PDF attachment to the address below:

CCH@njd.uscourts.gov

Note: If directed to return the completed packet to chambers, please do so and chamber's staff will forward the documents to the Human Resources office for processing.

Congratulations on your internship with the U.S. District Court for the District of New Jersey!

Emma C. Fernandez-Regan, Human Resources Manager

UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

Please read and follow all specific instructions on each individual form. If you have any questions, please contact Brian Kemner or David Rodriguez.

Forms List

1. **Employment Eligibility Verification – I-9**

   We are required to verify the eligibility of employees and interns to work in/volunteer services to the United States. You must complete Section 1 of the I-9 form and provide identification papers as given on the "List of Acceptable Documents" page. You can present either:

   - Any one document from list A; OR
   - Two documents, one from List B (identity) AND one from List C (eligibility)

   NOTE: Please provide a clear photo copy in PDF format of the identification documents as per instructions. All documents must be unexpired.

---

2. **United States Courts Appointment – AO 78A**

   Verify that all information is accurate. Type in your name as the Appointee. The Judge will sign as your Appointing Officer. You will sign as the Appointee. The Judge will also sign as the official administering the oath. For "Duty Station" please type in the Courthouse location of your Judge: Newark, Trenton or Camden. For "Entrance on Duty" type the first day of your internship.

---

3. **Acknowledgment of Gratuitous Services and Waiver Form**

   In Section A, please enter the period of your internship and the Judge that you will be interning for. Print name, sign, date at the bottom of the form and return.

---

4. **District of New Jersey Background Check Form**

   Answer all questions on this form and sign, date and return. NOTE: Provide a **clear** copy of your **valid** Driver's License. Complete Section B of this form **ONLY** if you are interning under your law school's Federal Work Study Program.

---

5. IT Policy

Review the attached policy, sign and return the acknowledgement form.

---

6. Personal Use of Government Envelopes, Supplies, and Telephone Equipment

Review the attached policy, sign and return the acknowledgment form.

Please review each form for completeness, accuracy and signatures.

Only return the completed forms NOT copies of the attached policies.

When returning the documents via CCH@njd.uscourts.gov, please include on the subject line your full name and the name of your Judge.

e.g. John Doe (Intern) - Judge Jane Miller

Employment Eligibility Verification

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

USCIS
Form I-9
OMB No. 1615-0047
Expires 08/31/2019

►**START HERE:** **Read instructions carefully before completing this form. The instructions must be available, either in paper or electronically, during completion of this form. Employers are liable for errors in the completion of this form.**

ANTI-DISCRIMINATION NOTICE: It is illegal to discriminate against work-authorized individuals. Employers **CANNOT** specify which document(s) an employee may present to establish employment authorization and identity. The refusal to hire or continue to employ an individual because the documentation presented has a future expiration date may also constitute illegal discrimination.

Section 1. Employee Information and Attestation *(Employees must complete and sign Section 1 of Form I-9 no later than the **first day of employment**, but not before accepting a job offer.)*

Last Name *(Family Name)*	First Name *(Given Name)*	Middle Initial	Other Last Names Used *(if any)*

Address *(Street Number and Name)*	Apt. Number	City or Town	State	ZIP Code

Date of Birth *(mm/dd/yyyy)*	U.S. Social Security Number	Employee's E-mail Address	Employee's Telephone Number
	☐☐☐ - ☐☐ - ☐☐☐☐		

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 boxes):

☐ 1. A citizen of the United States

☐ 2. A noncitizen national of the United States *(See instructions)*

☐ 3. A lawful permanent resident (Alien Registration Number/USCIS Number): _____

☐ 4. An alien authorized to work until (expiration date, if applicable, mm/dd/yyyy): _____
Some aliens may write "N/A" in the expiration date field. *(See instructions)*

Aliens authorized to work must provide only one of the following document numbers to complete Form I-9:
An Alien Registration Number/USCIS Number OR Form I-94 Admission Number OR Foreign Passport Number.

1. Alien Registration Number/USCIS Number: _____
OR
2. Form I-94 Admission Number: _____
OR
3. Foreign Passport Number: _____
Country of Issuance: _____

QR Code - Section 1
Do Not Write In This Space

Signature of Employee	Today's Date *(mm/dd/yyyy)*

Preparer and/or Translator Certification (check one):

☐ I did not use a preparer or translator. ☐ A preparer(s) and/or translator(s) assisted the employee in completing Section 1.
(Fields below must be completed and signed when preparers and/or translators assist an employee in completing Section 1.)

I attest, under penalty of perjury, that I have assisted in the completion of Section 1 of this form and that to the best of my knowledge the information is true and correct.

Signature of Preparer or Translator	Today's Date *(mm/dd/yyyy)*

Last Name *(Family Name)*	First Name *(Given Name)*

Address *(Street Number and Name)*	City or Town	State	ZIP Code

STOP *Employer Completes Next Page* STOP

Employment Eligibility Verification

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

USCIS
Form I-9
OMB No. 1615-0047
Expires 08/31/2019

Section 2. Employer or Authorized Representative Review and Verification

(Employers or their authorized representative must complete and sign Section 2 within 3 business days of the employee's first day of employment. You must physically examine one document from List A OR a combination of one document from List B and one document from List C as listed on the "Lists of Acceptable Documents.")

Employee Info from Section 1	Last Name *(Family Name)*	First Name *(Given Name)*	M.I.	Citizenship/Immigration Status

List A Identity and Employment Authorization	**OR**	**List B** Identity	**AND**	**List C** Employment Authorization
Document Title		Document Title		Document Title
Issuing Authority		Issuing Authority		Issuing Authority
Document Number		Document Number		Document Number
Expiration Date *(if any)(mm/dd/yyyy)*		Expiration Date *(if any)(mm/dd/yyyy)*		Expiration Date *(if any)(mm/dd/yyyy)*
Document Title				
Issuing Authority				
Document Number				
Expiration Date *(if any)(mm/dd/yyyy)*				
Document Title				
Issuing Authority				
Document Number				
Expiration Date *(if any)(mm/dd/yyyy)*				

Additional Information

QR Code - Sections 2 & 3
Do Not Write In This Space

Certification: I attest, under penalty of perjury, that (1) I have examined the document(s) presented by the above-named employee, (2) the above-listed document(s) appear to be genuine and to relate to the employee named, and (3) to the best of my knowledge the employee is authorized to work in the United States.

The employee's first day of employment *(mm/dd/yyyy)*: _____ ***(See instructions for exemptions)***

Signature of Employer or Authorized Representative	Today's Date *(mm/dd/yyyy)*	Title of Employer or Authorized Representative

Last Name of Employer or Authorized Representative	First Name of Employer or Authorized Representative	Employer's Business or Organization Name

Employer's Business or Organization Address (Street Number and Name)	City or Town	State	ZIP Code

Section 3. Reverification and Rehires *(To be completed and signed by employer or authorized representative.)*

A. New Name *(if applicable)*			**B.** Date of Rehire *(if applicable)*
Last Name *(Family Name)*	First Name *(Given Name)*	Middle Initial	Date *(mm/dd/yyyy)*

C. If the employee's previous grant of employment authorization has expired, provide the information for the document or receipt that establishes continuing employment authorization in the space provided below.

Document Title	Document Number	Expiration Date *(if any)* *(mm/dd/yyyy)*

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	Today's Date *(mm/dd/yyyy)*	Name of Employer or Authorized Representative

LISTS OF ACCEPTABLE DOCUMENTS
All documents must be UNEXPIRED

Employees may present one selection from List A
or a combination of one selection from List B and one selection from List C.

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.** A Social Security Account Number card, unless the card includes one of the following restrictions: (1) NOT VALID FOR EMPLOYMENT (2) VALID FOR WORK ONLY WITH INS AUTHORIZATION (3) VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)		**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 report of birth issued by the Department of State (Forms DS-1350, FS-545, FS-240)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa		**3.** School ID card with a photograph		**3.** Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
4. Employment Authorization Document that contains a photograph (Form I-766)		**4.** Voter's registration card		**4.** Native American tribal document
5. For a nonimmigrant alien authorized to work for a specific employer because of his or her status: **a.** Foreign passport; and **b.** Form I-94 or Form I-94A that has the following: (1) The same name as the passport; and (2) An endorsement of the alien's nonimmigrant status as long as that 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		**5.** U.S. Citizen ID Card (Form I-197)
		6. Military dependent's ID card		**6.** Identification Card for Use of Resident Citizen in the United States (Form I-179)
		7. U.S. Coast Guard Merchant Mariner Card		**7.** Employment authorization document issued by the Department of Homeland Security
		8. Native American tribal document		
		9. Driver's license issued by a Canadian government authority		
		For persons under age 18 who are unable to present a document listed above:		
		10. School record or report card		
		11. Clinic, doctor, or hospital record		
		12. Day-care or nursery school record		
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				

Examples of many of these documents appear in Part 13 of the Handbook for Employers (M-274).

Refer to the instructions for more information about acceptable receipts.

AO 78A (Rev. 09/15)

United States Courts Appointment

A

Judge's Staff: ✔ Yes ☐ No

U.S. District Court - District of New Jersey
(Name of Court)

_____ is appointed.
(Name of appointee - First, Middle, Last)
(Name will be on records as printed)

Judicial Intern (Position title) | _____ (Date of entrance on duty) | _____ (Duty station)

(Vice N/A ; Sep _____
(Previous incumbent) *(Mm/dd/yyyy)*

_____ (Signature of appointing officer)

_____ (Title of appointing officer)

(Note: Appointing officer, please indicate the grade or level recommended N/A)

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)

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

in _____ (City), _____ (State)

_____
(Title of official administering the oath)

_____
(Signature of official administering the oath)

(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.

Print | Save As... | Reset

Acknowledgment to Gratuitous Services and Waiver Form

(Interns/Externs/Volunteers Only)

A. I, _____, hereby declare that the services I will perform from approximately _____ /_____ /_____ to _____ /_____ /_____ in the capacity of a Judicial Intern for the Honorable _____ of the United States District Court for the District of New Jersey are to be rendered solely as a volunteer. I hereby waiver any claim or right to receive a salary or other compensation from the District Court in consideration for the performance of duties assigned by Judge _____. (Other than Work Study pay from my law school or university or other stipend from a source approved by my judicial officer).

B. I acknowledge that I am not entitled to receive civil service retirement credit or other related personnel benefits as a consequence of my 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 I retain no personal copyright privileges in any work product prepared by me in the course of my volunteer period. Finally, I recognize that information which I obtain, or to which I shall have access in the course of my volunteer period, is often of confidential nature, and I agree to preserve the confidentiality of such information.

C. Pursuant to The Guide to Judiciary Policies & Procedures, Chapter 310.10, The Code of Conduct for Judicial Employees applies to all employees of the judicial branch, including interns, externs and other court volunteers.

Canon 1:	A judicial employee should uphold the integrity and independence of the judiciary and of the judicial employees office.
Canon 2:	A judicial employee should avoid impropriety and the appearance of impropriety in all activities.
Canon 3:	A judicial employee should adhere to appropriate standards in performing the duties of the office, including avoiding conflicts of interest.
Canon 4:	In engaging in outside activities, a judicial employee should avoid the risk of conflict with official duties, should avoid the appearance of impropriety, and should comply with disclosure requirements.
Canon 5:	A judicial employee should refrain from inappropriate political activity.
Gift Regulations:	A judicial employee shall not, except as specifically permitted, solicit or accept a gift from any person seeking official action from or doing business with the employees court or office, or whose interests may be substantially affected by the performance of official duties.
Honoraria Regulations:	Judicial employees may not accept payment for an appearance, speech, or article, including a series of related appearances, speeches or articles related to official duties or where payment is made because of the employees official position.

A violation of these rules could result in a personnel action or, for certain offenses, civil and criminal sanctions under related statutes on conflict of interest. If you have questions after reviewing the information outlined, please contact the Human Resources Manager.

I agree to strive to preserve and protect an independent and honorable judiciary and observe the principles of ethical conduct as required by the Code of Conduct for Judicial Employees.

_____

Signature Date

_____

Name (Print) Date

Pursuant to the authority vested in the Director of the Administrative Office of the United States Court 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.

_____ _____

William T. Walsh, Clerk Date

UNITED STATES DISTRIC COURT
DISTRICT OF NEW JERSEY
William T. Walsh
Clerk

CRIMINAL HISTORY CHECK FORM (CCH)

PLEASE TYPE OR PRINT CLEARY

☐Law Clerk ☐Intern/Volunteer/Extern
☐Fellowship Program/Federal Work Study Intern ☐Clerk's Office New Hire

Judicial Chambers: _____

Length of Term: From_____/_____/_____ To_____/_____/_____

***SECTION B:** Interns & Externs only: If under a Federal Work Study Program or a Fellowship Program, please complete the following information.*

_____ _____ _____
Name of School Contact Person Contact Email

NOTE: The mandatory fingerprint process requires the full middle name of the applicant. If applicant only has a middle initial, please include the initial followed by "IO' (Initial Only). If the applicant does not have a middle initial, please write "NMN."

Please complete the following address information **as it appears on your Driver's License:*

Driver's License Number:_____State Issued:_____Expiration Date: _____

Full Name: _____ _____ _____
FIRST LAST MIDDLE NAME/MI

Current Address: _____

City/Town:_____State:_____Zip code: _____

Social Security Number:_____-_____-_____ Date of Birth (mm/dd/yyyy): _____ /_____ /_____

Contact number: (____)-_____-_____ Email address: _____

Have you ever been arrested? ☐Yes ☐No

If yes, please explain: _____

Have you ever been convicted of a crime? ☐Yes ☐No

If yes, please explain: _____

U.S. Citizen/Legal Resident? ☐Yes ☐No

If not a U.S. Citizen, please indicate country of citizenship: _____

Place (State/County) of Birth:_____

Gender: ☐Male ☐Female Race: _____

Height: _____ Weight: _____

Hair Color: _____ Eye Color: _____

Applicant Signature_____ **Date:** _____/_____/_____

Note: Please send this form <u>and</u> a photocopy or picture of your Driver's License to CCH@njd.uscourts.gov

Any false statements or omissions in this application may lead to a withdrawal of an offer of employment/internship, or termination of employment/internship.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MEMORANDUM OF UNDERSTANDING & ACKNOWLEDGMENT

COURT TECHNOLOGY POLICY

I, _____, have read and understand the Policy and Procedures for Computer, Internet and E-mail use. I agree to abide by this policy during my employment with the Court. I understand that any violation of this policy may subject me to disciplinary action.

_____ _____
Name (Print) Divisional Office

_____ _____
Signature Date

United States District Court
District of New Jersey

COURT TECHNOLOGY USE POLICY

Purpose: To establish guidelines for Court employees regarding the use of computers and other technologies provided by the United States District Court for the District of New Jersey (NJD).

Scope: These procedures will be observed by all NJD Court employees.

Effective: 2/2001 rev. 9/2009, 3/2010, 2/2011, 2/2012, 2/2013, 8/2015, 5/2016, 10/2017, 10/2018

Procedure:

Introduction

The information in this policy will inform court employees of current guidelines that govern the security and use of computers, networks and other technologies. All employees of the court who use or have access to computers and other technologies in the course of their duties are required to adhere to the guidelines presented in this document.

General Use of Computer Resources and Services

Government-supplied computer and telecommunications resources and services covered under these guidelines include, but are not limited to the following: workstations, laptops, netbooks, software, video conferencing, courtroom technology, fax machines, host computers (servers), all mobile devices (cell,PDA/Smart,Blackberry) and the use of internal or external networks and services accessed directly via the judiciary s private network or indirectly by remote access.

Funding to purchase technology is from tax revenue. These systems are the property of the federal judiciary. Knowing this, court employees have a greater responsibility to safeguard these systems and to exercise good judgment as to the appropriate use within the broad guideline of official business and to use them for their intended purpose, namely conducting court business.

All court systems, including hardware, mobile devices, applications, files and internet use and any other information technology related activity are subject to monitoring and are not private.

The Court understands that staff cannot completely detach themselves from their personal lives while they are at work. At times, and especially during emergencies, staff may need to use telephones, fax machines and computers for personal business. The incidental use of this equipment is permitted. Personal use should be kept to a minimum and it should not interfere with the work of the Court. Excessive use and/or abuse of these technologies for personal business may result in corrective action.

Physical Security

Computers and other devices need protection from physical hazards to avoid damage. Users should protect equipment by taking the following precautionary measures:

A. Do not place liquids or food on or around this equipment, especially keyboards;

B. Protect equipment, especially desktop and laptop computers, from dirt and dust when construction or other dust producing activities occur;

C. Use a surge protector or other suitable power line filter;

D. Secure your computer by logging off the network when you are away from your desk extended period. Password enabled screen savers that are included with windows should be used and should require a password.

E. Securing Laptop, Tablet and other Mobile Equipment: For those who have authorization to use court-owned laptop, netbook and mobile computers, special care must be taken. Laptops, netbooks and mobile computers are expensive and, due to their compact size, are susceptible to theft. For that reason, it is important to safeguard this type of equipment in your possession. This equipment should not be left out in the open for extensive periods of time. As with all systems, screen-saver password protection should be implemented. Laptops, tablets and other mobile devices should not be left in courtrooms unattended and in a vehicle in plain view. When laptops, tablets and devices are not being transported home for remote access/COOP purposes, the devices should be secured out of view, such as in a locked drawer, when not in use.

F. Damage to and/or theft of or loss of any equipment should be reported immediately to the IT Department. The Incident Response Plan should be followed.

If equipment is lost, stolen or destroyed through an employee s negligence, failure to provide adequate safeguards or willfully damage government property, the employee may be held personally liable for the cost of repair or replacement in accordance to Guide of Judiciary Policy Volume 16 555.20(e)(1).

Only Court issued equipment can be connected to the Court s network, do not connect equipment such as personal laptops, desktops, printers and wireless/non-wireless access points.

Access Control

Access control security measures are in place for the protection of the Court s information systems, NJD uses an identification and documentation process for authorizing access. No employee will be given system access without background check completion and employment confirmation from the Human Resources department. Further consent for specific access needs, is identified via a manager s approval by submitting a System Access Request form upon hiring, position or duty change. Access privileges are customarily defined based on an employee s job role. Chambers access is given based on consistent chamber needs (without a form). Any exceptions will require review by appropriate staff and will be documented.

Systems will be configured with non-privileged access for non-IT employees, this eliminates undesirable viruses, malware, software, and configuration changes from occurring on the Court s systems, only appropriate IT staff will have suitable privileged access to systems in order to execute their assigned duties.

Passwords

Passwords are a key to judicial information and infrastructure. It is the first line of security to ensure authorized access and legitimate utilization of our systems.

The following identifies practices for the creation, protection and aging of individual user passwords for all systems and electronic devices:

A. Change the default passwords on all systems and devices;

B. Forced change of passwords will be put into effect every 90 days or to system limitations;

C. Systems are set to password screen-lock after being idle for 30 minutes or to system limitations;

D. Passwords should be eight or more characters in length or to system limitations;

E. Passwords must contain at least four alphabetic characters and at least one numeric character; can only have three repeated characters in row; not start with special characters - - all subject to system limitations;

F. Passwords must not contain the user s account name or user s full name, or to system limitations; Should not be single meaningful words, family names, birthdays or simple alphanumeric sets (W Y , 12345) or system

limitations;

G. Password history is enabled on local domain file server access to prevent password reuse for five passwords; Other systems are set to limitations.

Additional Password Practices

Passwords should not be shared, written down or posted; Passwords should not be given to anyone; if your password is provided to a member of the IT staff for support activity, change your password as soon as the work has been completed; it is recommended that employee s use password vault software;

Do not insert passwords into email messages or other unsecure electronic communications;

Do not use the Remember Password feature of applications;

Users should report suspected password compromises immediately to the IT department and change the password immediately.

Internet Access

The Internet provides electronic access to a multitude of sites for obtaining information and conducting research. The Court provides employees with the equipment and the necessary browser software to use the Internet for court business. Therefore, court employees have an obligation to use the Internet in a responsible and professional way, conforming to network etiquette, customs and courtesies. When accessing the Internet, on or off duty, employees must adhere to the same code of ethics that governs all other aspects of judiciary employee activity and should not allow Internet activity to interfere with the performance of official duties.

The District of New Jersey does not have its own Internet Services Provider. Access to the Internet is provided by the Administrative Office of the U.S. Courts through gateways which are strategically located throughout the country. Providing Internet access to thousands of court employees is expensive. To protect and manage this investment, the Administrative Office has instituted various security and monitoring measures. Intrusion detection software is designed to safeguard the judiciary s information systems and to thwart hackers and other unauthorized users. This software has an added capacity too. It notes when large amounts of data pass through the gateways such as movie and music files. This type of traffic consumes a disproportionate amount of the network s capacity which can degrade the performance of the entire court network.

The Court typically blocks files and access to sites like steaming radio/video, music/videos, sexually explicit material, gambling sites, peer-to-peer sharing, chat rooms, instant messaging and the downloading of exe files, these items either pose extraordinary security risks or downgrade network performance.

All court users are encouraged to observe the following rules when using court-supplied

equipment and software for accessing the Internet:

A. Do not access Internet sites which may be inappropriate or reflect poorly on the judiciary. Unless case-related, creating, downloading, viewing, storing, copying and transmitting sexually-explicit or sexually-oriented materials is unacceptable and inappropriate and may be illegal in some cases. Internet sites capture the domain name of all sites accessing them and maintain a record of this information. It could be embarrassing to you and the Court if the judiciary s domain name (uscourts.gov) were found on the access records of inappropriate sites.

B. Do not log on to radio, video chat (ex. skype) and other broadcast services or download music and video files. Logging onto video or audio sites, such as broadcast services or radio stations, degrades the performance of the entire network. Downloading music files consumes significant disk space on local computers and may be a violation of copyright law. These services should be used for official purposes such as training.

C. Do not participate in chat rooms or use Instant Messaging (IM) software. There is court approved Instant Messaging software that can be used. Judiciary employees should only participate in Instant Messaging when directly relevant to their official duties and responsibilities. All others should be avoided. When participating in Instant Messaging, employees should not inadvertently give the impression of articulating official judiciary policy or positions. The Court locally blocks unapproved chat rooms and Instant Messaging.

D. Web-based document management, such as Google Docs, oho and iWorks, allows for collaboration and sharing of documents, known as cloud technology. Without purchasing word processing software, web services offer home users the opportunity to create word processing documents, spreadsheets, forms and more, the applications residing on the web server. With a purchased copy of Microsoft Office, you can use Office Web Apps.

Home users must keep in mind confidentiality and security implications of creating and sharing content. Collaboration on projects and documents is one of the perceived benefits of Web 2.0. Trusted brands, such as Google, may provide users with a level of comfort they would not have for other services. For U.S. Court users, Court documents and information should never be shared online at a vendor-hosted site with which the Judiciary does not have an agreement in place to obligate the third party to protect its data. This also includes sending Court documents and information via personal email.

E. Do not use the network connection for personal commercial purposes, private gain or illegal activities. 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).

F. Do not use the Internet to play games, this activity consumes bandwidth and affects system performance.

G. Be mindful that Internet sites keep logs of visitors. Court employees should only visit sites that are relevant to their official duties and responsibilities. The release of court user information by inappropriate sites would be an embarrassment to the courts.

H. Refrain from entering court e-mail addresses on web sites. Entering your court e-mail address on web sites increases your risk to receive viruses and spam.

Social Media

Emerging platforms for online collaboration are fundamentally changing the way we interact, offering new ways to engage with colleagues, friends and the world at large. Facebook, Twitter, You Tube, and MySpace. If you are a social media user, please adhere to the same code of conduct that governs the actions of all judicial employees. Do not post or discuss anything that is court-related. Violators will be subject to adverse action.

Viruses

Experts estimate that there are many programs in circulation which are designed to destroy or corrupt data. Some replicate themselves exponentially and fill up the available space on a hard drive. These are known as worms. Other viruses appear at some predetermined point in time and either change a file or eliminate it.

Viruses can infect a personal computer in different ways. Information which is down-loaded from a web site, ftp site or email can include a hidden virus program. Movable media, such as CDs and flash-drives used on a computer located outside of the office can be infected as well, particularly if it contains games or utilities. Viruses are imbedded into private e-mail attachments and can infect the Court s PCs.

Viruses can be very destructive. Recovering from them can be very expensive. To guard against viruses, we are instituting the following precautionary measures:

A. Avoid the use of removable media which contain files that have been copied from a personal computer located outside of the office.

B. Do not load any software, including games, screen savers, utilities or application software from home, which is not provided by the Court.

C. All personal computers have been furnished with virus protection software. If a virus is detected on your PC, please notify immediately a member of the IT Staff.

D. Viruses can be embedded in personal e-mail accounts and attachments. Knowing this, court staff should not access personal e-mail accounts using court-supplied equipment. Court staff should not open email or attachments received from people that they do not know in their court accounts.

Anti-virus software is mandatory on all judiciary computers, laptops, and servers, and non-judiciary owned computers that access judiciary networks, including virtual machines.

E-Mail

Electronic mail is the non-interactive communication of text, data and images between a sender and designated recipient(s) by systems utilizing telecommunications links. Electronic mail usually requires the sender and recipient(s) to enter a password as a precondition for access.

The electronic mail systems that are used by court staff are the property of the United States District Court for the District of New Jersey and are intended for official business. Employees should not expect their communications to be private, and should not use electronic mail for personal and/or confidential matters that are not intended for public disclosure.

When using e-mail, court staff should observe the following:

A. Use government e-mail appropriately. It is inappropriate to use government systems to send or receive e-mails containing greeting cards, political statements, jokes, pictures and other items of a personal nature. Chain letters or other unauthorized mass mailings, regardless of the subject matter, are inappropriate, because many are specifically designed to carry viruses.

B. Avoid sending large attachments unless required for official business. Video, audio 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 of infection by computer viruses.

C. Avoid checking personal e-mail accounts over the judiciary s network. Checking personal e-mail accounts could bypass virus scanners on the judiciary s mail servers, raising severe security risks locally and judiciary-wide. Sending sensitive judiciary information through personal web email accounts outside the judiciary network is also discouraged since the email accounts reside on a third-party server that does not afford the user sufficient security or privacy.

D. Do not use e-mail or the network connection for offensive activities. 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.

E. Beware of chain e-mail. Chain e-mail are messages which ask the recipient to send a letter to a number of others. This type of electronic traffic is an inappropriate use of the Court s network and can cause technical problems. Court staff receiving chain e-mail should print the message, turn it over to an immediate supervisor and then delete the message from the inbox. Staff originating chain e-mail may be subject to corrective action.

F. Look out for Phishing/Scam emails. A Phishing email is a fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity or person in an email. Email with a fake link or attachment is sent to unsuspecting users in an effort to solicit information or spread viruses. Never click on a link or attachment from someone you do not know even if it appears to be from valid address. Also, be wary of emails that appear to come from someone you know, but just do not look right.

Managing E-mail Accounts

Each court employee assigned an e-mail account has responsibilities for managing messages. Messages are generally saved and, therefore, accumulate in certain folders. Typically, these include the inbox, sent mail, trash, and special folders. Messages may also be saved to any folders created by the user. Messages consume disk space and excessive message storage can affect overall system performance.

To assist with the management of the Court s e-mail system, each employee is requested to perform the following:

A. Delete messages from the inbox, sent mail, special folders and trash folders as soon as possible.

B. Archive any messages that need to be saved for any length of time to your N drive.

IT Staff have been asked to monitor the excessive accumulation of email messages. They have been instructed to delete any messages that are over 90 days old and saved to the inbox, sent mail, special folders and trash folder.

Managing Server Files

Each court employee is assigned file server space and given access to shared directories (ex. Common drive) on the server. The file servers used by court staff are the property of the United States District Court for the District of New Jersey and are intended for official business. Employees should not expect their file content to be private and should not save files for personal

and/or confidential matters that are not intended for public disclosure.

When saving files in any area of the file server, observe the following:

A. Use government server space appropriately. It is inappropriate to use government systems to save files containing movies, music, pictures, jokes, political statements and other items of a personal nature.

B. Do not save movie, music or picture files to the server shared drives unless they are court-sponsored events. Court-sponsored videos or pictures will also need to be approved by the Clerk or Chief Deputy prior to posting.

Files consume disk space and excessive file storage can affect overall system performance, increase backup time and have a negative impact on Disaster Recovery situations. To assist with the management of the Court s servers, each employee is requested to perform the following:

A. Delete from work file directories, including shared drives, those that are over a year old and no longer in use and/or consider archiving important older files to CD or a flash-drive.

B. Refrain from saving movies, music and pictures to the Court s servers.

The IT staff has been instructed to monitor the excessive accumulation of files and to delete inappropriate files and assist employees in decreasing their work files to increase server performance.

Court Intranet/Internet Web Postings

The Court web sites provide easy electronic access to obtaining information. The IT staff has an obligation to ensure that the Court is represented in a professional way on the internal and external sites. All postings to either site must be approved by the Clerk, Chief Deputy or Systems Managers.

Remote Access

Access to the VPN/JPORT is limited to permanent employees of the U.S. Courts. Remote access users and teleworkers should adhere to the level of security as internal users noting that laptops and mobile devices are property of the U.S. Courts and should be used by Court employees only. All remote access users must review the VPN Policy and submit a VPN request form.

IT Security Awareness

Court employees are informed of their responsibilities regarding use of IT systems through court technology policies and procedures, internal controls guide, required IT Security

Awareness training for new employees, required annual IT Security Awareness training for existing employees and through further IT security awareness information disbursed via intranet or email. New and annual IT Security Awareness training is tracked by the Training Coordinator.

Violations of Policy

It is important that Court staff familiarize themselves with this policy. Any questions or concerns should be discussed with a supervisor, a manager and/or a member of the IT staff.

In addition to this policy, there are other local and Judiciary-wide policies and procedures that apply to the use of court-supplied systems and technology. Local policies are posted on the court s intranet site and the Guide to Judiciary Policies and Procedures can be found on the JNET.

Violations of policies may prompt corrective action resulting in a number of outcomes including a written warning, suspension, loss of computer privileges and/or, depending on the severity of the violation, involuntary separation. In some cases, the willful misuse of court-supplied technology may result in criminal prosecution.

Policy Review

This policy is reviewed and approved by the Director of IT annually to ensure the policy remains effective and applicable to NJD s local area network and adheres to industry best practices and national judiciary policy and guidance.

Exceptions

Exceptions to this policy will be formally documented, and periodically reviewed for on-going legitimacy in accordance with New Jersey District s IT security procedures.

UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

PERSONAL USE OF GOVERNMENT ENVELOPES, SUPPLIES, TELEPHONE AND EQUIPMENT

ACKNOWLEDGMENT AND MEMORANDUM OF UNDERSTANDING

I, _____, acknowledge receipt of and have
PRINT NAME

read the policy on "Personal Use of Government Envelopes, Supplies, Telephones and Equipment."

I understand and agree to comply with this policy. Failure to do so may subject me to corrective action and/or adverse action.

_____ _____
Signature Date

_____ _____
Print Name of Judge Interning for Courthouse location

§ 3.32 Personal Use of Government Property - Photocopies, Supplies, Postage and Telephones

Employees are not permitted to use government property or supplies for their personal use. Employees will be required to reimburse the government at fair market value for photocopies made for personal use. Employees will also be required to reimburse the government at fair market value for any supplies either taken from the office or put to personal use. Employees are prohibited from using government supplied envelopes, postage meters, or postage stamps for personal use (18 U.S.C.§1719).

Due to the vast number of business telephone calls, both outgoing and incoming, the use of government telephones for personal calls will be limited to emergency or very important calls only. Personal calls should be made during a break or a lunch period, if possible. Family members and friends should be informed of this provision.

The policy of this office prohibits employees from charging any personal long distance telephone calls on government telephones except in a dire emergency, and, then, only with the approval of the Clerk of Court or the Chief Deputy. Pursuant to the Administrative Office policy, employees who make an authorized personal call must reimburse the Government for any long distance telephone calls made on government telephones and are also liable for a 10% federal excise tax.

Excessive use of government-owned phones and/or abuse of the above-mentioned government property, equipment and supplies is unacceptable and may be subject to corrective and/or adverse action.