

Third Circuit Court of Appeals Technology Guide

Table of Contents

Introduction	3
1.0 Systems Management and Monitoring.....	3
1.1 User Desktops	3
1.2 User Support.....	4
1.3 Data Replication.....	4
2.0 Security	4
2.1 Physical Security	5
2.1.1 Desktop Equipment	5
2.1.2 Mobile Devices.....	5
2.1.3 Portable Storage Devices.....	5
2.2 Data Integrity and Security	5
2.3 Network Security.....	6
2.3.1 Passwords	6
3.0 Remote Access.....	7
3.1 From a Personal Device	7
3.2 From a Public Device.....	8
3.3 Telework.....	8
3.4 Remote Access Support	9
4.0 Court Software Applications.....	10
4.1 Email/Messaging	10
4.1.1 Email Policy.....	11
4.2 Case Management	12
4.3 Word Processing	13
4.3.1 Metadata	13
4.4 Computer Assisted Legal Research (CALR)	14
4.5 Trusted Resources and Information Online (TRIO)	14
4.6 Court of Appeals Web-based Resources.....	14
4.7 Software Updates	14
5.0 Personal Software Applications	15
6.0 Internet Use	15

7.0 Appropriate Use and Social Media	16
7.1 Third Circuit COA Appropriate Use Policy.....	16
7.2 Prohibited or Limited Activity	17
7.2.1. Blocked Activity	17
7.2.2. Advertisements.....	17
7.2.3. Prohibited Activity	17
7.2.4. Offensive Content	17
7.2.5. Limited Activity	17
7.3 Social Networking.....	17
8.0 Interns/Externs	18
9.0 WiFi.....	18
10.0 New Staff	18
10.1 Notification of Start Date	18
10.2 Standard Setup.....	19
10.3 First Day	19
11.0 Extended Leave.....	19
12.0 Separation.....	20
12.1 Email and Contacts	20
12.2 Preservation of Email and Folders.....	20
A1 Glossary	21

Introduction

Information technology (IT) is central to the work of the courts. Its effective operation is a high priority, since all aspects of court work involve IT.

The rapid pace of technological change includes the proliferation of personal devices and their introduction into the workplace. Employees are expected to have a high level of aptitude and comfort with technology.

This guide is intended for all Third Circuit Court of Appeals (COA) employees and explains the basic design and operation of the judiciary's IT infrastructure and security framework, and provides an explanation of the standard software applications and services in use.

All employees must read this guide and agree that they understand and will abide by judiciary and COA policy regarding the use of IT. These policies are based on the judiciary's Code of Conduct, which each employee is required to follow. (*Code of Conduct for Judicial Employees*)

1.0 Systems Management and Monitoring

The federal judiciary operates over a network that is comprised of a national Wide Area Network (WAN) which is managed and maintained by the Administrative Office of U.S. Courts, and Local Area Networks (LANs) maintained by each individual appellate, district, bankruptcy, probation and pretrial office that connect users to the WAN and out to the Internet. The COA maintains its own LAN in each of our locations.

The judiciary's network is a shared resource. Judiciary IT staff at both the national and local level proactively manage the network to ensure adequate performance for all users and adequate security for the judiciary's information systems. The work of the courts is the priority, and part of the management process involves monitoring network activity to ensure appropriate use. This may result in restrictions or prohibitions on some types of employee activity.

1.1 User Desktops

The standard user desktop operates using the Windows operating system. A number of enterprise applications, discussed in more detail below, are installed on each user's desktop. Because these applications are essential to the work of the COA, there are restrictions on users' ability to add or modify applications on their desktop. ***To ensure security and software operability, desktop activities are tracked.***

The work of the COA is confidential and there is personally identifiable information stored in the case management system and in human resource systems and records. ***To safeguard the integrity and confidentiality of this information, user activities on the network are monitored and logged.***

Virtual Desktops

Most COA users work from a “virtual” desktop. In the office, your virtual desktop is accessed using a small appliance called a ‘zero client.’ Nothing is stored on these appliances, they have no moving parts, and are easily swapped out when they need to be replaced. This is the same desktop you access remotely using a mobile device or a home computer.

1.2 User Support

User support is available from the COA IT Help Desk. All calls placed are logged and routed to the appropriate staff to address the problem. Your call can often be more quickly routed if you are able to specify the category or type of problem you are having when you place a call – Word is slow when saving or retrieving a document; I get an error message when *sending* an email but not when *replying to an email*; etc. If you are getting an error message, being able to report the exact wording of the message is very helpful.

Users are encouraged to do some initial checking or testing on their own to more precisely identify or narrow down a problem, including checking with coworkers to see if they also have the problem.

1.3 Data [Replication](#)

The COA uses a high availability data model that replicates data in real time so that your work is always backed up and available from several sources. There may be times when you accidentally move or delete a file you are working on. When that occurs, the IT Help Desk should be able to recover or restore the missing file.

2.0 Security

Information security is a primary concern for the federal courts. When you are connected to the network, your failure to follow the security measures in this section puts at risk information and data not just for the COA, but for all federal courts around the country.

2.1 Physical Security

2.1.1 Desktop Equipment

We ask that you safeguard COA computer equipment from physical damage and loss. Be careful with beverages and food. In addition, please do not move your equipment or reroute cabling. If you need assistance with relocating equipment, please contact the IT Help Desk.

2.1.2 Mobile Devices

If you have a COA-owned portable device such as a notebook computer, a tablet or a smartphone, you are responsible for the security of that device. You should have the device with you at all times unless it is secured at your home. Do not leave a COA-owned device unattended, even briefly. While the COA's mobile environment is designed to minimize the possibility that confidential COA information would be stored on the device, it is still a possibility. ***You may be required to reimburse the government for the loss of a device that occurs through failure to follow this guidance.***

If you have confidential court information and documents stored on a personal device you should follow the same precautions outlined above. You are responsible for the security of confidential court information that you have stored on a personal device.

2.1.3 Portable Storage Devices

Use of flash drives and other portable storage devices to store or transfer confidential COA information is strongly discouraged. The convenience associated with the small size of these devices also makes them susceptible to loss and theft. Although these devices may be encrypted, the judiciary does not use a standard [encryption](#) tool.

2.2 Data Integrity and Security

You are required to safeguard the confidentiality and integrity of COA data and your work product. Moving COA work product from the secure network to personal devices or Internet storage is strongly discouraged. Choosing to work outside of the COA's network places the burden on you to ensure that COA work product is secure and backed up, and that court data is purged from any personal devices when the work is complete.

If you do move COA work product and data to a personal device or to Internet cloud storage, you are responsible to take appropriate steps to safeguard it. The COA does

not endorse a specific [encryption](#) tool, but if you are moving files using a flash drive or through file storage or personal email on the Internet, you should encrypt the files.

You are also responsible for backing up any files that you work on outside of the COA's network. Backing up files to a local hard drive or device is not recommended, but if you have already made the decision to work on COA files outside of the COA's network, you need to regularly back up your work.

Once your off-network work is completed, you are responsible for deleting and purging any backup copies of court work product from personal devices. You need to use something more than the delete option, since even fragmented files can be recovered fairly easily from a device. *(There are third-party software tools available for this purpose, but an acceptable approach is to delete the file, then use the Disk Clean-up and Disk Defragmentation tools from the System Tools menu in Windows.)*

2.3 Network Security

There are national policies in place that establish security requirements protecting access to COA information. The judiciary operates on a private, nationwide network that is segregated from the Internet. Access to this network requires user authentication with a password. Each court, including the COA, also maintains its own local network and password access. Some applications also require separate login.

2.3.1 Passwords

The federal judiciary has a national password policy that users must follow. Passwords must:

- (1) be at least 8 characters long;
- (2) include upper and lower case letters;
- (3) include at least one number and one non-alphanumeric character (e.g., %, #, \$, etc.);
- (4) not be a proper name, place, or something personally associated, such as a birth date; and
- (5) not be the same for all systems and access.

Accountability

Passwords provide you with authorized access to the network and systems. You must not write down passwords where they can easily be found and you should never share your password. National policy requires that you use a password-protected screen saver or session lock set to activate after 15 minutes of inactivity on your desktop. ***Any inappropriate activity or***

unauthorized access through use of your password will be attributed to you.

It is each user's responsibility to safeguard his or her passwords. If you believe your password has been compromised or obtained by others, it is your duty to immediately change your password and notify the IT Help Desk.

Unauthorized Access

You should not use anyone else's password. Attaining, or attempting to attain, access to information that you have not been given password access to will be considered unauthorized access. ***Unauthorized access could result in disciplinary action, legal action, or both.***

Guidance

There is guidance available to help you create passwords that are sufficiently complex yet still easy to remember. You can also have different passwords for different systems that all follow the same scheme, making them easier to manage. If you need assistance, contact the IT Help Desk. ([Password Strategies](#))

Change Intervals

It is recommended that you change all of your passwords at least once every six (6) months.

3.0 Remote Access

Some employees are provided with access to the COA's network from the Internet. If authorized, you will be given a password that allows you to use either the virtual private network ([VPN](#)) or [JPORT](#) to access your COA desktop and resources. This access is secure, and since your work product never leaves the COA's network, it is backed up and safeguarded from corruption and unauthorized access.

Employees can also directly access their COA email account from the Internet through [WebMail](#). Using your Lotus Notes password, you are able to run Notes from a web browser. Although WebMail is very close in functionality to the Notes desktop client, there may be some functions that are not supported. [Remote Access Options Chart](#)

3.1 From a Personal Device

Virtual Private Network (VPN)

Separate instructions for use of the [VPN](#) are provided for both Windows and Apple iOS. The [VPN](#) operates using software installed on your device or built into the operating system. ([VPN Instructions](#))

Use of the VPN requires software on your computer, so the more flexible and preferred approach is to use JPORT on personal as well as public devices. The levels of access are the same.

Junos Pulse

Like the [VPN](#), Junos Pulse must be installed on your device. It also uses your [VPN/JPORT](#) user name and password to authenticate you to the court's network. ([Junos Instructions](#))

3.2 From a Public Device

JPORT

[JPORT](#) provides similar functionality to the [VPN](#) client but operates through a browser and requires no special software on your device. There are separate instructions for [JPORT](#) use. Both [VPN](#) and [JPORT](#) use the same user ID and password. However, [JPORT](#) can be accessed securely from any device on the Internet, including a public PC at a hotel or library, or the device of a friend or family member. ([JPORT Instructions](#)) ([JPORT for the Mac](#))

WebMail

[WebMail](#) works like [JPORT](#) except that you are limited to Notes once you connect. WebMail uses your Lotus Notes email account as your username and your Notes password rather than your [VPN/JPORT](#) user name and password. WebMail can be accessed from any computer on the Internet. <https://webmail.uscourts.gov/>

3.3 Telework

The court has separate guidelines for telework eligibility and home office requirements. Authorized teleworkers can use the [VPN](#) or [JPORT](#) to access their work. Teleworkers can also use Cisco's soft phone software, obtained from the Help Desk, that is installed on the telework computer and connects directly to the COA's phone system through the Internet. This allows the teleworker to make, receive and forward phone calls and retrieve voicemail without tying up a local phone line or a cell phone.

Currently the federal judiciary has a contract for Symantec antivirus software that allows installation of the software on personal devices while employed by the courts. You can contact the Help Desk for installation instructions.

Microsoft has a program that allows court employees to purchase Office for Windows or Mac at a significant discount. Information is available on the Microsoft website under 'Home Use Program.'

3.4 Remote Access Support

Working remotely involves use of personal devices and Internet access and introduces a number of variables beyond the control of COA IT staff. The IT Help Desk can assist with any issues with set up and configuration by the IT staff and can assist in identifying possible causes of problems related to personal devices and your Internet Service Provider (ISP).

Connectivity

The IT Help Desk can assist with connectivity issues as they relate to the authentication process, but the Help Desk cannot troubleshoot telework computer problems related to changes made to the local computer. The IT Help Desk can verify that the login process is attempted at the network gateway and any details of a failed attempt, but the number of issues that could prevent getting at least that far in the connection process are potentially vast. The IT Help Desk can provide general guidance for troubleshooting, but it is the responsibility of the teleworker to explore and resolve problems associated with Internet access.

Printers

If teleworkers want to print at the telework location they need to ensure they have a working printer and can provide the printer driver to the IT staff. While the IT Help Desk can provide support to ensure that drivers are properly installed, other printer problems are beyond the scope of what the IT Help Desk can assist with. ([Printing through JPORT](#))

Performance

There are a number of factors that can affect performance and the IT Help Desk can assist with some, but not all, of them. Before connecting to the COA's network, teleworkers should verify that their Internet connection is performing acceptably. If teleworkers are not sure about the quality of their Internet connection, they should perform local testing.

Chronic performance problems could relate to the age of the teleworker's computer, the number of users and types of applications installed on the teleworker's computer, a virus or Trojan on the teleworker's computer, or a service problem with the Internet Service Provider (ISP). All of these problems would need to be addressed by the teleworker.

WiFi

If teleworkers use [WiFi](#) to connect their computer and/or printer to a local network, it is the teleworker's responsibility to ensure that adequate security has been set up on

the wireless router. Teleworkers must know and maintain their local wireless authentication code and how to set up a device on the wireless network. The IT Help Desk cannot provide assistance in connecting to the local [WiFi](#) connection or securing it.

Remote Assistance

While the IT Help Desk can attach to the teleworker's remote desktop to assist with problem-solving, the IT Help Desk cannot connect to and make changes on the teleworker's computer.

Security

The IT staff can provide Symantec anti-virus software and instructions for its installation and use. Teleworkers can purchase another anti-virus application if they so desire. It is the responsibility of teleworkers to apply and maintain adequate security on their telework computer. (§[330.30.20 Guide to Judiciary Policy](#))

Teleworkers are required to use an adequate firewall. Use of either the VPN or JPORT eliminates the need for the teleworker to have a separate firewall. However, if teleworkers choose to perform COA work without being connected via the VPN or JPORT, they must use a local firewall on the telework computer. Because of the number of options and the potential complexity of firewalls, the IT Help Desk cannot provide assistance with setting up and maintaining local firewalls. (§[330.30.30 Guide to Judiciary Policy](#))

4.0 Court Software Applications

4.1 Email/Messaging

The Judiciary uses IBM's integrated messaging suite of software -- Lotus Notes for email and calendaring, Sametime for instant messaging (IM), and Connections for internal social media.

Notes

There are three different versions of Notes available to COA users: (1) the desktop client, (2) WebMail, which is web-based and accessed via the Internet through <http://webmail.uscourts.gov/>, and (3) Traveler, which can be installed on your personal smartphone or tablet ([Traveler installation instructions](#)). Each version has different functionality, especially in terms of calendar access and features.

In addition to personal Notes calendars, each COA unit and many chambers use shared office calendars. Access to multiple calendars can be set up with bookmarks

in Notes. The Help Desk can assist with instructions for setting this up. ([Notes information](#))

Sametime

Sametime can be used to instant message anyone in the judiciary and is accessible from the Notes client. Sametime cannot be used to IM outside of the judiciary's private network. Instructions for set up and use of Sametime are available. If you need assistance you can contact the Help Desk. ([Sametime information](#))

Connections

Connections is a judiciary-wide social media tool with many communities covering all areas of court work and interest. Most communities are open, meaning anyone can join, although some are closed and require either a specific invitation or permission to join. ([Connections information](#))

4.1.1 Email Policy

COA email is official correspondence. National judiciary and COA policies and practices for written communications apply. COA employees should remember that an email message is easily copied or forwarded without the sender's knowledge. If you have questions about your COA unit's guidelines for communications, talk to your unit head.

- (1) Conduct. Email users are expected to conduct themselves in a professional manner and should refrain from using profanity or obscenities. The email system is for business use and is not a forum for soliciting personal goods and services, promoting charities, or other discussions of personal viewpoints. A level of civility and decorum befitting the judiciary should be observed at all times.
- (2) Files Attached to Email. Any file attached to an email message is automatically scanned for viruses. If you are notified that an attachment may be infected, contact the IT Help Desk immediately.
- (3) Maintenance. The number of stored email messages should be kept to a minimum. An excessive amount of email both impacts storage space and decreases system performance. It is your responsibility to delete old email messages and empty your trash folder.

Messages with large attachments should be saved out of email to the network after initial review. Users whose mailboxes have become excessive in size will be contacted by IT staff and directed to reduce the number of messages saved.

- (4) Security. A person who gains access to your email account will be able to read all of your email and may send messages to others in your name. Each user is responsible for the security of his/her email account. Passwords should be changed frequently. Your computer must have a password-protected screen saver when you are away from your desk. This will ensure that your email will not be available to unauthorized users in your absence.
- (5) Retention. COA email is centrally hosted and maintained. All email is archived nationally on tape for a period of three (3) years. Any email is retrievable for that period of time.

4.2 Case Management

The federal judiciary has its own family of case management systems called [CM/ECF](#). There are bankruptcy, district and appellate versions of [CM/ECF](#). These systems are web browser-based. Court staff are provided user IDs and passwords by the Clerk's Office.

[CM/ECF](#) is the electronic docket and official record for the COA. All documents are filed electronically or scanned and stored electronically as part of the docket. The electronic version of documents are the official version of the documents. Attorneys file electronically from the Internet. Training on the use of [CM/ECF](#) is provided by the Clerk's Office.

Chambers and Mediation utilize CM/ECF for document management purposes and they each have private docket reports to monitor transactions made by their offices.



There are two types of docket entries in [CM/ECF](#), private and public. Private docket entries are for use by chambers and COA staff only and are not available to the public. Public docket entries appear in black, private docket entries are in blue type for the Clerk's Office and green type for the Legal Division and are distinguished by the word INTERNAL (see below).

04/03/2012

INTERNAL NOTE: A call was made to Alexander Robbins, Esq. requesting an electronic addendum (EMA)

When providing information to parties and the public, you cannot disclose any information from private docket entries.

Documents and information filed under seal should not be made available to the public without express authorization. Below is an example of a docket entry for a sealed motion. A lock appears for the document and the 'SEALED' text is displayed upon selecting a sealed event.

01/15/2013   ECF FILER: SEALED Motion filed by Appellant John Doe 2 in 12-1697, Appellants ABC Corp, stay Pending the filing of a petition for certiorari. Certificate of Service dated 01/15/2013. [12-169

Documents filed in Social Security and Immigration cases are automatically restricted and viewable by court staff and case participants. The restriction does not apply to orders, judgments, and opinions filed in these cases.

Court staff may also view the public docket in [PACER](#).

4.3 Word Processing

The word processing application used by the COA is Microsoft Word. This is not a judiciary-wide standard; some courts use Word and others use WordPerfect. The COA also still has a number of legacy documents in WordPerfect.

The COA has established font and format standards for its opinions. There is also a standard for the naming of opinion files.

4.3.1 [Metadata](#)

[Metadata](#) is embedded information in a document that is generally hidden. It can reveal the creator of a document, track changed and edited text, and keep a history of everyone who has edited the document.

Information contained in metadata stays with the document unless it is removed. [Metadata](#) can stay with the file even when it is converted from one file format to another. Many court documents are converted from Word to Adobe [.pdf](#) format. Unless [metadata](#) is removed, it will be accessible in a published document such as an opinion, when it is made publically available. All court opinions are posted on the COA's Internet site.

The [metadata](#) in court documents such as orders and opinions could reveal confidential information. There are separate instructions on how to remove [metadata](#) – in most cases it is done via a setting in Word or Acrobat. ([How to Remove Metadata](#))

If you are preparing a document that will be made available outside of the COA you are responsible for ensuring that all metadata has been removed. If you have any questions, contact the IT Help Desk.

4.4 Computer Assisted Legal Research (CALR)

The judiciary has contracts with LEXIS and Westlaw. User accounts for Westlaw and LEXIS are managed by the Third Circuit Library. The Library will issue you a user ID and password. The Library also has access to other databases. A list of these databases can be found on their website, [TRIO](#).

4.5 Trusted Resources and Information Online (TRIO)

The Third Circuit Library provides a wealth of resources on its TRIO website, accessible directly (<http://trio3.circ3.dcn:81/>), or from the Third Circuit intranet page. The site also includes access to Legal Subject Guides, the Library's catalog, and Third Circuit digital archives.

4.6 Court of Appeals Web-based Resources

The Court of Appeals has both a public-facing Internet site (www.ca3.uscourts.gov) and an intranet site (www.ca3.circ3.dcn) available only from the secure network. The intranet site contains court policies, standards, and work-related links and resources. There are also links to the [JNET](#), the Administrative Office's internal web site, and to other court units – district, bankruptcy, probation – within the Third Circuit. There are also links to resources discussed in this guide, including JPORT, WebMail and iNotes.

Leave/Time and Attendance System

The COA uses custom leave tracking and time and attendance systems. These systems are web-based and accessed from the COA intranet page.

4.7 Software Updates

As a general rule, you should not install software updates for applications on your desktop or the operating system. The IT staff manages this process and will apply updates as needed. However, there may be times when the IT staff will notify you to install an update and you will be provided with instructions. If you have any questions about updates, please call the Help Desk.

5.0 Personal Software Applications

Staff members, law clerks, and judicial assistants are not permitted to install personal software on a COA desktop unless they receive express permission from their judge or unit head. Unless the personal software has a work-related purpose, it will generally not be allowed.

Personal software includes games, instant messaging, and applications for cataloging music, photos or video. Personal software can create technical problems with court applications and use significant network bandwidth and storage space. The judiciary may also incur a legal liability for unauthorized copying of files or software even if the copy is used for official business.

6.0 Internet Use

The Internet is an important work resource and is available to all COA users. Access is through the judiciary's private network and use is subject to monitoring and restrictions. Your use of the Internet must adhere to the same code of ethics that governs all other aspects of judiciary employee activity. While personal use of the Internet is not prohibited for COA employees, limited and appropriate use is expected as explained in section 7.1.

National policy prohibits access to gambling and gaming sites. There are also restrictions in place regarding excessive use of network bandwidth. Activity that is not prohibited based on content may still be prohibited because of the bandwidth resources that are used. Access to streaming video and audio directly impacts the ability of all other users on the building network to get their work done. For example, a COA user in Philadelphia watching NetFlix can impact performance for all COA and district court judges and staff in the courthouse.

Access to prohibited sites as well as activity that creates excessive use is monitored. ***When you are connected to the court's network through JPORT or VPN your activity is also monitored, whether or not you are on your remote desktop.*** The COA IT staff is notified by the Administrative Office of the activity and required to investigate and address the problem. COA unit heads are notified of all inappropriate Internet use and of excessive use when notification to the user by the IT staff is not sufficient to remedy the problem.

When accessing personal Internet-based email from a computer connected to the COA network, any viruses or malicious software associated with a message could infect court systems. Please avoid opening suspicious messages and, in particular, any attachments to suspicious messages. Call the IT Help Desk if you need assistance in identifying suspicious messages.

You should also use care when browsing to websites that could be infected or a possible repository of malware. The antivirus software on each court desktop and server will catch most malware, but often not the newest malware. If you have any concerns about a website, do not use a computer attached to the court network to access it.

7.0 Appropriate Use and Social Media

7.1 Third Circuit COA Appropriate Use Policy

The Third Circuit COA policy follows the guidance from the Judicial Conference of the United States on appropriate use of the Internet.

Users may not use the Internet:

- (1) To send data files or email over the Internet that contains any discriminatory or offensive statements referring to race, creed, color, sex, or sexual preference;
- (2) To make unauthorized commitments or promises of any kind that might be perceived as binding the judiciary;
- (3) To send data files or email over the Internet that concern ongoing investigations or pending litigation. The Internet is not a secure means of transmission and can cause a case or investigation to be compromised should the data be intercepted and read by an unauthorized party;
- (4) To send data files or email over the Internet that could reflect poorly on or cause embarrassment to the judiciary;
- (5) For commercial purposes or private gain;
- (6) For improper usage or distribution of software or information that includes copyright violations;
- (7) For illegal activities; or
- (8) For political activities.

7.2 Prohibited or Limited Activity

7.2.1. Blocked Activity

In accordance with U.S. Judicial Conference policy, access to certain types of activity is blocked. Currently blocked at the national level are gambling and gaming sites. In addition to these sites, the COA blocks sites that are designated as malicious because they are used to support and propagate malware.

7.2.2. Advertisements

Unsolicited advertisements embedded in web pages can utilize significant bandwidth and propagate malware, and may be blocked by the COA.

7.2.3. Prohibited Activity

In addition to sites that are blocked, COA policy prohibits visiting adult entertainment/pornographic and fetish web sites, hate sites, and sites that portray graphic depictions of violence.

7.2.4. Offensive Content

Content not otherwise included in the categories blocked or prohibited above may also be prohibited if it is determined that the content and the office setting in which it is accessed combine to create a hostile work environment.

7.2.5. Limited Activity

All other activity of a personal nature should be limited and is permitted only to the extent that such activity does not generate excessive network traffic and is done in accordance with COA office policies about engaging in personal activity while at work.

7.3 Social Networking

Court employees are expected to honor the confidentiality of the judiciary in all forms of communication, including social networking. You are expected to observe the confidentiality policy of the COA. Anything that would be inappropriate to share about the COA or your work with others is inappropriate to share on a social networking site of any sort, *even if you are sharing anonymously or under a pseudonym*.

For additional guidance on the use of social media you can read the advisory opinion from the Judiciary's Committee on Codes of Conduct. ([Advisory Opinion No. 112](#))

8.0 Interns/Externs

Interns and externs are not considered court employees and their access to court network resources is limited.¹ Generally, interns and externs are not provided email accounts. Chambers may have designated intern workstations set up with generic accounts that will provide network access, but interns and externs are not given network accounts that can be used from personal devices.

The COA [WiFi](#) has a separate channel intended for intern and extern use with personal devices such as tablet and notebook computers. This channel provides limited access to Third Circuit Library research materials ([TRIO](#)) and the Internet, allowing interns to access WestLaw and LEXIS. There is no direct access to the COA network.

The Code of Conduct for Judicial Employees specifically applies to interns and externs. Interns and externs are bound by the COA's social media and confidentiality policies regardless of whether they are provided access to email and Internet resources.

9.0 [WiFi](#)

The COA provides [WiFi](#) access in all chambers, courtrooms, libraries, and staff offices. We broadcast two channels. The first channel, dcn_gtwy, the national [WiFi](#) channel, is for judges and employees only. This channel provides full access to the secure network and is available at any judiciary location around the country that supports [WiFi](#).

The second channel, 3COA_Intern, is available at any court location within the Third Circuit that provides [WiFi](#). The password for the intern channel is managed and maintained by the Third Circuit Library. In addition to providing access for interns and externs, court employees are permitted to connect personal devices – tablets, smartphones, notebooks – to the intern network. Employees are able to access the secured court network by using their [VPN/JPORT](#) account to connect securely from a personal device.

10.0 New Staff

10.1 Notification of Start Date

The IT staff should be notified of new staff at least two weeks prior to the expected start date. This allows for sufficient time to provide and set up a telephone handset and a desktop, and to set up software, accounts, and access.

¹ Automation and Technology Committee of the U.S. Judicial Conference, March 1999

The hiring unit should provide information about the level of access to data and applications the new hire will need using the New Employee Request form. This form should also include special email accounts or groups the individual should be added to.

10.2 Standard Setup

Depending upon the specified level of access to data and applications requested, each new employee generally will be set up with network access, which includes a VPN/JPORT account, an email account, and a 'home' file directory. You can use the links in this document to set up services like VPN access or Traveler for email, or you may call the Help Desk.

10.3 First Day

On your first day, you should verify that your accounts have been set up, that applications installed on your desktop are working, and that you have access to the data you need. **You should also change any default/initial passwords you were given.**

Decisions about some services or applications, like Sametime instant messaging or access to certain email accounts, may be made on a chambers-by-chambers or unit-by-unit basis. These services are not part of the default setup, but can be added by request with the appropriate approval.

11.0 Extended Leave

If you will be out of the office on extended leave you should discuss how you want to handle email and network and system access with your supervisor. Your accounts can be suspended or remain active. We recommend that if you will not be working during your leave, that access to the network and applications like CM/ECF be suspended.

If you want to stay in contact with what is going on you may keep your email account active. However, if you don't anticipate spending time answering emails, you should activate the out-of-office feature to let senders know your status.

12.0 Separation

12.1 Email and Contacts

Before leaving the COA you should go through your email account and, working with your supervisor, forward or save any work-related email or attachments. You should not leave active work-related communication and work product in your email account when you leave.

Email in your COA Notes account is the property of the Court of Appeals. You may take your email with you when you leave the COA only with the written permission of your judge or unit head.

You are free to take your personal contacts with you, and they can be exported as v-card files. The IT Help Desk can assist you with this.

12.2 Preservation of Email and Folders

Email accounts of departed employees will be disabled on the termination date for the employee, but maintained for six (6) months. At that point, the unit head will be asked to authorize the deletion of the account. In the judiciary's centralized email environment, maintaining large numbers of dormant accounts organization-wide creates a significant drag and cost on the system.

Note: Although the account will be deleted from the live email system, the account and messages it contains remain on tape archive for an additional three (3) years.

Under special circumstances, such as short notice of departure, at the direction of a judge or unit head, the email account of the departing employee may be redirected to another employee or the account may be monitored for a period of time. When this is necessary, an out-of-office message should be added to the account that notifies email senders the individual is no longer with the COA and information about new points of contacts.

A1 Glossary

Glossary

CM/ECF	Case Management/Electronic Case Files is the standard case/docket management system used by the federal judiciary. The system supports electronic filing by attorneys via the Internet. As denoted by the name, the official record for a case is stored electronically in CM/ECF.
DCN	Data Communications Network, the “intranet” platform used to transmit information within the federal judiciary.
Encryption	Process of converting data into a format that can only be read or deciphered by authorized users. A key is needed to encrypt and decrypt data.
Firewall	Set of related programs that protects a private computer network from users of other networks. (The term also implies the security policy used with the programs.) An organization with an intranet that allows its workers access to the wider Internet may install a firewall to prevent outsiders from accessing its own private data resources. It also controls what outside resources its own users may access.
JPORT	Short for Judiciary Portal, JPORT provides access to the judiciary’s private network (DCN) through any device connected to the Internet. Unlike VPN access, JPort is accessed through a web browser and does not require any software to be installed on the computer. Once connected to JPORT, the user most typically connects to their desktop remotely. https://jport.uscourts.gov/
Metadata	Refers to "data about data." Metadata is descriptive information about a document such as who created the document, who reviewed it, and what changes or comments they made. This information is embedded in the document file and stays with the document unless stripped out.
PACER	Public Access to Court Electronic Records is the system used by attorneys and the public to access court records and to file documents with the court. This system is accessible from the Internet and ties into the CM/ECF system. A fee is charged for PACER access. Link to PACER
PDF	Portable Document Format, developed as a standard file format for Internet documents. The primary advantage of PDF files is that they are viewable and printable on all computers without disruption to formatting or layout. PDF “text files” are written or converted via software directly from word processing formats into PDF format. PDF “image files” are converted from

their original paper form to PDF via a scanner. They require significantly more memory and are generally not searchable.

- Replication** Process of backing up data by copying information from a primary server to a separate server. This is done so that the secondary server may be used as a resource in the event of an unexpected outage or loss of data (e.g., natural disaster, damaged data).
- VPN** The Virtual Private Network provides a secure, encrypted tunnel, across the Internet to the judiciary's internal network (DCN). VPN use requires a user name and password. This is the same password used for JPORT. VPN access is supported by software installed on a Windows computer or via a service built into the Apple operating system on an Apple computer.
- WebMail** Judiciary WebMail uses IBM Mobile Connect (IMC) to provide access similar to JPORT with the exception that the user only has access to Notes.
<https://webmail.uscourts.gov/> *Note that Webmail replaces JРАН.*
- WiFi** A play on the term Hi-Fi – high fidelity – WiFi provides wireless access to the network. A device with wireless capability is required and the SSID – Service Set Identifier – and password for the WiFi channel must be set up on the device. You must be within range of a wireless access point to be able to access WiFi, and moving out of range once connected will cause the connection to drop.

**United States Court of Appeals
for the Third Circuit
TECHNOLOGY USER MEMORANDUM OF AGREEMENT**

As a user of IT network resources and services of the United States Courts,

1. I understand that failure to sign this acknowledgment will result in denial of access to the judiciary's network (DCN).
2. I acknowledge that I have read the Technology Guide for the United States Court of Appeals for the Third Circuit.
3. I understand the policies outlined in the Guide and I agree to abide by them.
4. I understand that I am responsible for all actions taken on the network and in email accounts that have been assigned to me and will use these accounts in accordance with the provisions set out in the Guide.
5. I will not attempt to gain unauthorized access to computers, networks or telecommunication systems nor attempt to view or use information for which I am not specifically authorized.
6. I understand that I am responsible for maintaining the current level of security available on my desktop connected to the judiciary's network.
7. I understand that I am responsible for the proper use, care and reasonable protection from damage or loss of equipment that I use and will return it to the court in good condition, excluding normal depreciation, at the end of my period of employment.
8. I promise not to take any actions which will jeopardize the security of the judiciary's network or other automated information systems after my departure from employment with the court.
9. I acknowledge my responsibility to conform to the requirements and conditions set forth in this agreement, and I will abide by all applicable policies.

I acknowledge that I have read and understand the policies and requirements in this guide and agree that I will comply with them during my employment with the Court of Appeals.

Name

Date

Court Unit
