

# **COMPUTER SECURITY HANDBOOK**

*for End Users*



*U.S. District Court  
Northern District of Ohio*

*Geri M. Smith, Clerk of Court  
December 2015*

## TABLE OF CONTENTS

INTRODUCTION .....	<a href="#">1</a>
GENERAL USE OF COMPUTER RESOURCES AND SERVICES .....	<a href="#">1</a>
SYSTEM MONITORING .....	<a href="#">1</a>
PHYSICAL SECURITY .....	<a href="#">2</a>
Protecting Your Computer .....	<a href="#">2</a>
Data Protection .....	<a href="#">2</a>
PASSWORDS .....	<a href="#">2</a>
Length and Composition .....	<a href="#">2</a>
Security .....	<a href="#">2</a>
Creation and Maintenance .....	<a href="#">2</a>
Westlaw/Lexis .....	<a href="#">2</a>
REMOTE ACCESS .....	<a href="#">3</a>
Remote DCN Access .....	<a href="#">3</a>
Lotus Notes .....	<a href="#">3</a>
INTERNET ACCESS .....	<a href="#">3</a>
Electronic Mail .....	<a href="#">4</a>
Other Internet Services .....	<a href="#">4</a>
Acceptable Use of the Internet .....	<a href="#">4</a>
Unacceptable Use of the Internet .....	<a href="#">4</a>
Instant messaging .....	<a href="#">5</a>
Social Media .....	<a href="#">5</a>
Cloud Services .....	<a href="#">5</a>
USING WIFI NETWORKS .....	<a href="#">6</a>
SOFTWARE .....	<a href="#">6</a>
Copyrighted Software .....	<a href="#">6</a>
Demonstration Copies of Copyrighted Software .....	<a href="#">6</a>
Shareware .....	<a href="#">6</a>
Court-Developed Software .....	<a href="#">6</a>
Privately-owned Software .....	<a href="#">6</a>
VIRUSES/MALWARE .....	<a href="#">7</a>
Possible Signs of a Virus .....	<a href="#">7</a>
What to do if you suspect a virus: .....	<a href="#">8</a>
Techniques for Avoiding Viruses .....	<a href="#">8</a>
What is Malware: .....	<a href="#">8</a>
Signs of Malware are: .....	<a href="#">8</a>
Protect against Malware .....	<a href="#">8</a>
EMAIL POLICY .....	<a href="#">9</a>
Conduct .....	<a href="#">9</a>
Bulletin Boards .....	<a href="#">9</a>

<b>Files Attached to Email</b> .....	<b><u>9</u></b>
<b>Maintenance</b> .....	<b><u>9</u></b>
<b>Security</b> .....	<b><u>9</u></b>
<b>COURT-PROVIDED MOBILE DEVICES</b> .....	<b><u>10</u></b>
<b>Physically Secure the Device:</b> .....	<b><u>10</u></b>
<b>COURT-OWNED COMPUTERS IN PRIVATE RESIDENCES/LAPTOPS</b> .....	<b><u>10</u></b>
<b>BRING YOUR OWN DEVICE, USE OUR DATA</b> .....	<b><u>11</u></b>
<b>COMPUTER SECURITY AWARENESS TRAINING</b> .....	<b><u>11</u></b>
<b>USER MEMORANDUM OF AGREEMENT</b> .....	<b><u>12</u></b>

## INTRODUCTION

To protect the Data Communications Network (DCN), "Operating Guidelines" have been implemented which provide the framework for computer security in the U.S. District Court Northern District of Ohio. This handbook was written to provide users with a description of the security practices required by this Court. The information contained in this publication will raise awareness of computer security, define the responsibilities of the user, assist users in recognizing potential problems, and provide guidance to the end user if a compromise in security is suspected.

All DCN users are required to adhere to the security guidelines discussed in this document. The Court, via General Order No. 97-36, *Computer Usage, Electronic Mail and Internet Policy*, adopted these security guidelines. Additionally, the Court has decided that every court employee will be required to sign the "User Memorandum of Agreement" contained in this handbook. These guidelines apply to judges, chambers staff, including law clerks and externs. They also apply to all Clerk's Office, Probation and Pretrial Services employees, volunteers and externs who use the DCN.

## 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: file servers, standalone computers, laptops, software, e-mail, and the use of internal or external (including commercial) networks and services accessed directly via the judiciary's private network (the DCN).

Telecommunications resources include: telephones and other desktop instruments, telephone system processors and related equipment and software, mobile devices, special system features, like voice mail and conference calling, long distance calling and other telecommunication services.

These resources are provided for official Court business to be used to assist the employee in the performance of assigned duties. Since no two employees will use these resources in exactly the same way, each user will have to exercise individual responsibility and judgment as to appropriate use within the broad guideline of "official business." While incidental, occasional and limited personal use is not categorically prohibited, such use should not unduly interfere with official duties or be damaging to the Court.

In addition, fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be sent by e-mail or other form of electronic communication or displayed on or stored in any court-provided computer. Users encountering such materials should immediately report the incident to their supervisor.

## SYSTEM MONITORING

Computer and telecommunication systems are subject to monitoring for the technical aspects of those systems and their usage by assigned court employees. Those employees are expressly forbidden to monitor or make available in any fashion the content of correspondence, electronic mail, draft opinions or orders, research activities, confidential data or confidential databases, without specific authorization from the Court.

Documents created and maintained on networked systems are assumed to be created in the course of performance of official duties and may be official records. As part of the routine backup schedule, files kept on these systems are duplicated daily. Should official need for access to an employee's files or electronic mail arise, it will be provided upon request by appropriate management authority.

## PHYSICAL SECURITY

Protecting Your Computer. Computers need protection from physical hazards to avoid damage to the computer or loss of data. Users should protect equipment such as the computer unit (CPU), zero client, monitor, keyboard, and printer by taking the following measures:

- ▶ Do not place drinks (or any liquids) on or around the PC/zero client or keyboard, and avoid dropping crumbs or any foreign materials on the keyboard.
- ▶ Protect the PC/zero client and keyboard from dirt and dust, particularly when construction or other dust producing activities occur.
- ▶ Use a surge protector or other suitable power line filters.
- ▶ Avoid areas susceptible to water damage.
- ▶ Secure the workstation by invoking a password protected screen saver or logging off the network when you are not present.
- ▶ Maintain mobile devices in secure locations whenever they are not in use.

### Data Protection

All files stored on your H:, S: or O: network drives are replicated to other servers during business hours. Remaining network files are replicated from 6:00pm to 7:00am daily. If a file is inadvertently deleted from a network drive by the user, the IT department may be able to recover the document. In those instances, contact the help desk at your location for assistance.

## PASSWORDS

Length and Composition: All passwords shall be at least (8) characters long and shall consist of a combination of upper and lower case letters, numbers and special characters such as #, \$, %, ^. Passwords should never be easily guessed (names, names of a relative or friend, hobbies, or birth month).

Security: In no event should passwords be recorded on paper and left in an accessible place. Passwords are to be kept confidential and should not be shared with employees in the office or with individuals outside the office.

Creation and Maintenance: For some applications, such as CM/ECF, passwords will be provided to you. For network and email accounts, employees choose their own passwords that conform to this Handbook. You will be prompted to change your network password every 90 days. If specified, email passwords will automatically synchronize with the network password when changed. Passwords can not be reused.

Westlaw/Lexis is accessed directly via their website. The Circuit Library is responsible for providing user accounts for Westlaw access. Accounts are only issued to court staff who have work-related purposes for conducting legal research. The library also coordinates

training in the use of these applications and assists users in assuring that effective search strategies are being employed.

## REMOTE ACCESS

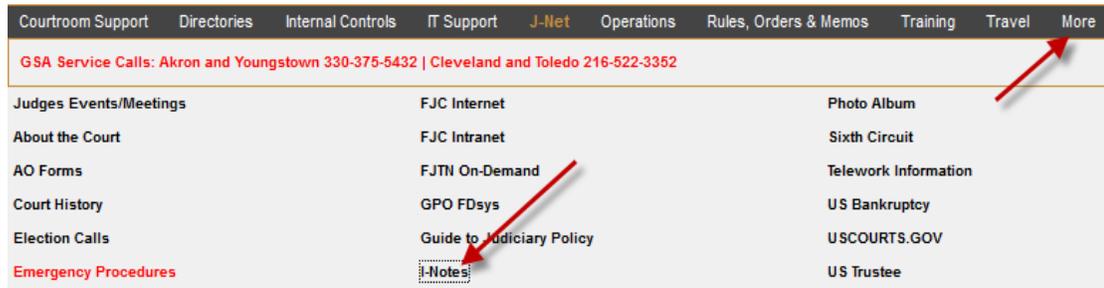
The Judiciary provides secure connections options to access the Court remotely: JPort ([jport.uscourts.gov](http://jport.uscourts.gov)); Lotus Webmail ([webmail.uscourts.gov](http://webmail.uscourts.gov)); Lotus traveler for mobile devices and the Cisco VPN client.

Remote DCN Access: Remote access to the DCN is provided through JPORT and a VPN account. JPORT allows judiciary users to connect to the DCN from any trusted computing device with an internet browser and connection. It provides secure access to an authorized user's office desktop. Instructions for using JPORT can be found on the intranet at the following link

<http://intranet.ohnd.circ6.dcn/home/training/desktop-application-support/remote-access-vpn/>

Lotus Notes: Remote access to Lotus Notes is available through INotes from within the DCN, or Webmail ([webmail.uscourts.gov](http://webmail.uscourts.gov)) from outside the DCN.

INotes can be accessed via the More button on the home page of the court's intranet.



Lotus Webmail allows judiciary staff access to their Lotus Notes email from any computer with internet access and a compatible browser. Instructions for using can be found here: [http://support.sdso.ao.dcn/support/LN/IBM\\_MobileConnect.aspx?group=Em](http://support.sdso.ao.dcn/support/LN/IBM_MobileConnect.aspx?group=Em)

## INTERNET ACCESS

These guidelines apply to all Internet services accessed using computer resources of the judiciary in accordance with General Order No. 97-36 *Computer Usage, Electronic Mail and Internet Policy*. These services include, but are not limited to, electronic mail, Web browsers, Telnet, and File Transfer Protocol (FTP). Employees who are authorized to use these services must make sure that they use the Internet safely and productively, and not in any way that could compromise the interests of the judiciary.

Access to the Internet is possible through the DCN. As part of the security system of the DCN's Internet gateway, a log is kept of all Internet activity passing through the DCN. This log is monitored for improper use at two gateway locations, Ashburn, VA, and San Diego, CA. In addition, if an individual accesses an Internet site or sends an electronic message through the DCN's Internet gateway, the fact that this activity originated from the United States Courts will be known by the receiving site or party. Inappropriate access could therefore be an embarrassment to the judiciary.

*Electronic Mail:* Any employee with a Lotus Notes account may use that account to send and receive Internet electronic mail provided that they follow the "acceptable use" provisions outlined below.

It should be noted that Internet mail is not secure. Messages can be read or broadcast without the knowledge or consent of the author. Users should not expect the messages they send or receive via the Internet to be private. Internet mail is also unreliable. Delivery and delivery times are not guaranteed due to unpredictable intermediary system and network outages and slowdowns. Users should not rely on Internet mail for time-sensitive communications or guaranteed delivery.

Large messages, messages with large attached files, or messages sent to large numbers of recipients are discouraged.

The Judicial Conference of the United States IT Security Policy 2006-1 states that access to personal web email accounts from within the judiciary's private data communications networks is strongly discouraged.

*Other Internet Services:* Access to Internet services other than electronic mail will only be made available to employees at the direction of a judicial officer or unit executive. Only those specifically authorized may use these services.

*Acceptable Use of the Internet:* Employee access to the Internet must adhere to the same code of ethics that governs all other aspects of judiciary employee activity. Employees may not use the Internet for other than authorized activities. While incidental, occasional and limited personal use is not categorically prohibited, such use should not unduly interfere with official duties or be damaging to the Court.

*Unacceptable Use of the Internet:* Employees are specifically prohibited from using the Internet for the following purposes:

- 1) Distribution of unauthorized statements regarding agency policies or practices;
- 2) Making unauthorized commitments or promises of any kind that might be perceived as binding on the Court or an agency thereof;
- 3) Transmitting confidential information, except as required for the performance of official duties;
- 4) Using subscription accounts or commercial services that are not expressly authorized;
- 5) Hosting an unauthorized web site;
- 6) Sending or displaying messages or pictures that are of an obscene or sexually explicit nature as defined in *Miller v. California* 413 U.S. 15, 23 (1972);
- 7) Using the network connection for commercial purposes or private gain;
- 8) Making or distributing unauthorized copies of copyrighted software, images, or text;
- 9) Using the network for illegal activities;
- 10) Using Court owned or created materials on unauthorized web sites.

Improper use or distribution of information is also prohibited. This includes copyright violations such as software piracy. The judiciary may incur a legal liability for unauthorized copying of files or software even if the copy is used for official business.

Employees should show respect for intellectual property and creativity by giving appropriate credit when files or portions of files are used while carrying out official duties.

Employees should be mindful of procurement sensitive information and should not transmit it over the Internet.

Employees should refrain from any practices which might jeopardize the judiciary's computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.

*Instant messaging.* The judiciary has selected Lotus Sametime as its secure, enterprise-wide IM solution. Other means of instant messaging such as Skype, Yahoo Messenger or AOL travel in clear text over the Internet, where their content—including sensitive judiciary or personal information—is potentially not secure and prohibited from use.

*Social Media.* The popularity of social network sites (Facebook, Google+, Twitter, YouTube and LinkedIn) and the open exchange of personal information associated with their use create a tempting environment for abuse. Further, as the privacy settings of popular sites are subject to change, be careful not to share any sensitive judiciary information on these sites.

- ▶ follow codes of conduct for judicial personnel
- ▶ do not identify yourself as a court employee
- ▶ do not reveal information about your whereabouts or that of any other court personnel, especially judges
- ▶ do not discuss confidential or sensitive information obtained as a result of working at the court
- ▶ do not divulge the date or location of judicial programs or meetings
- ▶ do not post pictures or personal information about judges or judiciary employees without their express consent
- ▶ do not post pictures of courthouses or other judiciary buildings

*Cloud Services.* The challenge when using mobile devices is the ability to remotely store and access files across devices. Freely available cloud services, such as Dropbox and Google Docs provide the ability to access files from any internet-connected device but are discouraged from use as they carry risks. Judiciary information should not be entrusted to third party cloud services unless there is a formal agreement to do so. Any information leaving judiciary systems is no longer secured by the judiciary.

The judiciary provides a private cloud service environment within the DCN called IBM Connections <https://connections.ao.dcn> to save and update documents. Users can access their files from any internet-connected device while at work or with a VPN account, at home or traveling.

## USING WIFI NETWORKS

The Court provides secure wireless access for court-provided devices only. Wireless access for the public and all non-court equipment is provided through the Attorney Wireless network–OHNDATTYW. Before using any public WiFi networks, please consider the following:

- ▶ use a secure wifi network (i.e. vpn, mifi, web, wpa, wpa2 encryption)
- ▶ send information to fully encrypted websites
- ▶ look for https at the beginning of the web address
- ▶ turn off the feature to automatically connect to available wifi connections
- ▶ public wireless networks are not secured by the judiciary
- ▶ when finished, disconnect from the network

## SOFTWARE

All software, no matter what type as described below, must be installed either directly by the IT department or with their knowledge and assistance. This is to ensure that any software used by employees on court-owned equipment is compatible with existing computer systems, properly installed, maintained, used and upgraded, free of any computer virus, and properly licensed. Software installed on court-owned equipment that does not comply with these guidelines will be removed by the IT department.

Copyrighted Software. Copyrighted software must not be reproduced, except as permitted by the terms and conditions of the contract under which it was purchased. All applicable laws must be obeyed and the use of pirated software is prohibited.

Demonstration Copies of Copyrighted Software. To avoid contract violations and to ensure that all software is obtained from legitimate sources, individual users are not authorized to accept demonstration software. Demonstration or trial software may only be obtained through normal procurement channels prescribed by each court unit.

Shareware. Shareware allows a user to try out software before paying a license fee. Since it is similar to demonstration software the same policies apply to its testing, purchase and installation as described above.

Court-Developed Software. Software developed by the Administrative Office or by a local court unit may be distributed directly to court employees by the IT department or the AO. All such software must be scanned for viruses prior to installation. The IT department should be contacted before installation.

Privately-owned Software. In general, employees are discouraged from using personally owned software on Government equipment. If the judicial officer or unit executive deems it in the best interest of the court to allow personally owned software to be installed on court-owned equipment:

- 1) Authorization should be granted in writing by the judicial officer or unit executive showing justification.

- 2) Employees not following these procedures may be held personally liable for violations of copyright laws and may be subject to the applicable penalties.
- 3) The employee is responsible for notifying the IT department when the software is no longer needed so that it can be properly removed from the equipment.
- 4) It is possible that, after installation, this software could be erased, or otherwise made unusable in the course of regular maintenance or upgrades by the IT department. To ensure that the software is not totally lost, the employee is responsible for keeping a proper backup copy in accordance with the license agreement.

## **VIRUSES/MALWARE**

The term “virus” is generically used to refer to any malicious computer program, but that classification is quite broad. Technically, viruses are codes that attach themselves to files and, when the files are opened, copy themselves onto other files. “Worms” are programs that copy themselves across networks without begin attached to a file. “Trojans” are a class of computer threats that appear to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen and control the computer. Any of these classes of computer codes can compromise security, corrupt data or even destroy computer hardware. They can be transmitted on executable programs, word processor documents or other seemingly innocuous files. A user may not know that a virus is present until months or years after the infection takes place. Only up-to-date, sophisticated virus detection software can reliably cure and prevent infection by computer viruses.

The judiciary has licensed anti-virus programs for use on all of the judiciary's PC's, including laptops and machines used by employees at home. All PC's and virtual desktops have this software installed, and are managed through the network for updates to virus signature files. IT personnel must be contacted at the first indication (or suspicion) of a virus.

Users should be able to identify the possible signs of a virus and identify what steps to take if a virus is suspected.

### *Possible Signs of a Virus:*

- ▶ PC is sluggish or locks up
- ▶ Popup windows appear
- ▶ Files are corrupted
- ▶ Unexpected messages
- ▶ New dates appear
- ▶ Files grow
- ▶ Files are lost
- ▶ Disk is unusable
- ▶ Strange messages appear on the monitor
- ▶ Hard disk crashes
- ▶ Memory capacity decreases

### *What to do if you suspect a virus:*

- ▶ Stop using your PC.
- ▶ Write down error message or description of a problem and what you were doing when you realized something was amiss.
- ▶ Stop using the infected workstation and turn off the computer.
- ▶ Immediately alert the IT department.
- ▶ Once the virus is removed, stay alert for possible reinfection.

Techniques for Avoiding Viruses:

- ▶ Ensure that all files are scanned for viruses before they are copied to your local hard drive or the network. Make certain that all executable files have been scanned and approved for use before first use (see Software).
- ▶ All disks or flash drive devices that leave the work area (i.e., work at home) or are obtained from an outside source should be scanned before being used in the workplace. Protect your data by making periodic backups, label all CD/disks/flash drives containing your data carefully and completely, and store CD/diskettes/flash drives in a secure location.

What is Malware:

Malware is a catch-all term referring to any malicious software designed to harm or gain unauthorized access to a computer system or the information on it. Malware attacks often include numerous delivery strategies to deliver malicious software, such as tricking users into opening infected email attachments or visiting corrupt websites.

Malware can be introduced onto a system in a number of ways. It can be downloaded through the unwitting actions of a user (e.g., clicking on a malicious link), or by a user visiting an infected web site. Malware can also be intentionally introduced by anyone who has access to the system, such as a disgruntled employee or a hacker.

Signs of Malware are:

- ▶ System slows down.
- ▶ Won't shut down or restart.
- ▶ Displays pop-up ads or web pages you didn't expect.
- ▶ In some cases, there may be no signs of infection at all

Protect against Malware:

- ▶ Be mindful of what you are clicking on and downloading
- ▶ Restrict pop-up ads
- ▶ Don't click on links in spam or pop ups that claim to offer anti-virus or anti-spyware software
- ▶ For smartphones and tablets, avoid clicking on links to untrusted sites and especially downloading applications from them
- ▶ Don't use untrusted CDs, DVDs, or USB drives

## EMAIL POLICY

The email policies contained in this handbook are for general use, please refer to General Order No. 97-36, *Computer Usage, Electronic Mail and Internet Policy*.

Users are reminded that email is official correspondence and each unit's normal policies and practices for other written communications applies. Keep in mind at all times that an Email is easily copied or forwarded to anyone without the sender's knowledge.

*Conduct.* Email users are expected to conduct themselves in a professional manner and should refrain from using profanity and/or obscenities in any electronic communication. The email system is not a forum for soliciting goods and services which are not directly related to official business.

*Bulletin Boards.* Bulletin board messages are used to display messages to the entire courthouse and should be used for posting court house-related functions. Each court unit has its own bulletin boards which can be used to post messages to in-house staff.

*Files Attached to Email.* Any file attached to an email message that contains an executable program (.exe) is filtered at the gateways and stripped from the email message before it is delivered.

*Maintenance.* It is the user's responsibility to delete and archive old email messages on a routine basis. As part of regular email maintenance, messages in the Trash folder are automatically deleted after 2 days. For most users, email messages older than 1 year will be automatically archived to an archive folder within Lotus Notes. Instructions for archiving and deleting email messages can be found on the intranet under IT Software Support.

*Security.* Each user is responsible for the security of their email account and should password protect upon minimizing or exit email when not preparing or reading messages. Employees are not to read other employee's email without prior permission.

You should change your email password when your network password is changed to keep them synchronized.

Ensure that your computer is logged off before you leave, or protected by screen blanking software that requires a password to reactivate to ensure that your email will not be available to unauthorized users in your absence.

## **COURT-PROVIDED MOBILE DEVICES**

Judiciary users should take vital steps in protecting their devices which in turn protects judiciary systems. A secure mobile device fortifies a strong judiciary system. Court-provided mobile devices such as an ipad/iphone are registered with AIRwatch which affords the court the ability to perform a remote wipe should the device become stolen. Here are some practices to consider for a more secured mobile device:

- ▶ Use encryption to keep portable data secure in transit.
- ▶ Turn off Bluetooth when not being used.
- ▶ Connect to only secure Wi-Fi networks and disable the mobile device when not in use.
- ▶ Configure mobile devices securely.
- ▶ Use a password protected screen lock on all the devices.
- ▶ Follow local incident reporting procedures if court-issued devices are lost or stolen.
- ▶ Only download apps from trusted sources.
- ▶ Avoid storing sensitive data on laptops or other mobile devices.

### *Physically Secure the Device:*

- ▶ Use a security cable for laptops when away.
- ▶ Don't leave laptops or phones alone in a car in plain sight unattended.
- ▶ Don't leave court devices unattended in public areas (e.g., airports, restaurants).

## **COURT-OWNED COMPUTERS IN PRIVATE RESIDENCES/LAPTOPS**

The purchase of PCs for permanent installation in private residences is prohibited by the Judicial Conference Committee on Judicial Improvements. However, court-owned cyclically replaced PCs may be used. (A cyclically replaced PC is one that has been removed from regular use due to age, condition, or obsolescence.)

Upon determination by a judicial officer or unit executive that it is in the best interest of the judiciary for an employee to use a cyclically replaced PC at home for official business, and provided that equipment is available, it may be provided under the following conditions:

- 1) The employee must sign a Property Receipt for the equipment acknowledging that it is for use in the conduct of official business, is responsible for its proper use, care and reasonable protection from damage or loss, must acknowledge their responsibility for any cost resulting from damage to or loss of the equipment due to negligence or carelessness, and must acknowledge that the judiciary is not liable for damages to an employee's personal or real property due to use of the court-owned computer in a private residence.
- 2) Software for the computer must be installed and used in accordance with the applicable licenses.
- 3) The approving office is responsible for maintaining an inventory of the equipment and for seeing that it is returned when the employee no longer needs it, when it malfunctions, or when the employee leaves court service.
- 4) The authorization to use the equipment should be reviewed annually by the IT department.

- 5) While the IT department will install appropriate software and provide set up instructions, the employee is responsible for setting up, maintaining, and removing the equipment from his/her residence.

## **BRING YOUR OWN DEVICE, USE OUR DATA**

While it is acceptable to bring your own device to work, typically to access email, data, and applications, you have the responsibility to protect judiciary information. Personally owned devices are permitted to connect to the court's public wireless network only—OHNDATTY. The IT department will provide assistance if necessary with setting up access to court email on your device. Personally owned devices that may be used for court purposes must follow the same guidelines outlined under Court-Provided Mobile Devices above. You are responsible for the ongoing maintenance of your device to ensure proper security measures are applied.

## **COMPUTER SECURITY AWARENESS TRAINING**

Users are the first and best line of protection from compromise of data on judiciary systems. Most breaches of computer security are attributable to computer users. This means that computer security rests in the hands of the users of computer systems. You are essential to providing security to the data and the machine entrusted to you.

New technologies are increasing computer security risks. Networks, telecommuting, mobile communications and portable computers mean that important, sensitive data is being moved and is at greater risk. Valuable information is now more vulnerable since it is mobile accessible, and more exposed to risk.

Each of the previous sections of this handbook describe the critical areas that you need to address to improve computer security. It is the responsibility of each employee of the U.S. District Court Northern District of Ohio to put the standards described in this handbook into action to protect the sensitive and mission critical information of the court.

To ensure that all employees keep current as technology continues to change, the IT department will provide annual computer security awareness training. At anytime, however, IT Security Awareness brochures are available for your reference on the JNET at the following location:

<http://jnet.ao.dcn/information-technology/security/training-and-awareness>

To ensure that you are aware of your security responsibilities, and to certify that you have received the most recent policies and procedures, you will be required to sign the Computer User Memorandum of Agreement. A copy of this appears at the end of this handbook.

The security of our systems requires the vigilance and commitment of each and every computer user. We thank you for your careful attention and dedication to this critical task.

**United States District Court  
Northern District of Ohio  
USER MEMORANDUM OF AGREEMENT**

As a user of the Data Communications Network (DCN), I acknowledge my responsibility to conform to the requirements and conditions established by this document.

1. I understand that failure to sign this acknowledgment will result in denial of access to the DCN.
2. I understand that the DCN is an unclassified network. I will not introduce, store, pass or process classified data on the network.
3. I understand the policies outlined in this Computer Security Handbook and I agree to abide by the Handbook.
4. I understand that I am responsible for all actions taken under my account. I will not attempt to "hack" the judiciary network or any other network or computer on the DCN or attempt to gain access to data for which I am not specifically authorized.
5. I understand that I am responsible for maintaining the current level of security available on my workstation connected to the DCN.
6. I acknowledge my responsibility to use the DCN **ONLY** for authorized purposes.
7. I acknowledge my responsibility to ensure that restricted information is not publicly disclosed and to immediately report suspected violations of this regulation.
8. I acknowledge my responsibility to immediately report to my supervisor and, subsequently the IT department, any contact with individuals in which illegal or unauthorized access is sought to sensitive information or when I become concerned that I may be the target of actual or attempted exploitation.
9. I acknowledge my responsibility NOT to download or install executable software from any source onto the DCN without prior authorization from management and/or the IT department. I recognize that I must ensure that any files or software I am authorized to receive have been subjected to approved virus protection measures.
10. I understand that all telecommunications and automated information systems are subject to monitoring to ensure proper functioning, to protect against improper or unauthorized use or access and to verify the presence or performance of applicable security features or procedures, and for like purposes. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in these systems by the user. If monitoring reveals possible evidence of criminal activity, such evidence may be forwarded to law enforcement personnel. I expressly consent to such monitoring. I understand that the IT department is responsible for such monitoring.

11. I understand that I must ensure that all equipment is returned to the court in good condition at the end of my period of employment, and I promise not to take any actions which will jeopardize the security of the system after my departure.
12. I acknowledge my responsibility to conform to the requirements set forth in this agreement, and I will abide by all applicable policies. Failure to comply may result in denial of access to the DCN and that, if necessary, such violations will be reported to the proper authorities.

Name: \_\_\_\_\_ Court Unit: \_\_\_\_\_

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

\_\_\_\_\_  
*Employee's Signature*

\_\_\_\_\_  
*Date*

\_\_\_\_\_  
*Supervisor's Signature*

\_\_\_\_\_  
*Date*

cc: Court Unit Personnel Record