ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

AO MANUAL

Volume 9: Information Technology

Chapter 1: Overview

§ 110 General

This volume contains policies and guidance on information technology (IT) for the AO.

§ 120 Applicability

Except where specifically noted, the policies set forth in this volume of the *AO Manual* apply to every AO workforce member who is responsible for one or more user accounts or an AO IT service or system. In other words, they apply to all AO workforce IT "users," a term that includes:

(a) all AO employees;

(b) employees detailed from other governmental agencies or courts;

(c) temporary workers;

(d) contractor personnel (subject to the terms of their AO contracts);

(e) interns (paid or unpaid) and others providing volunteer services; and

(f) vendors or consultants who have access to an AO IT system or service.

§ 130 Authority, Delegations, and Responsibilities

§ 130.10 Department of Technology Services

The AO Director has assigned responsibility to manage the AO's technology program to the Department of Technology Services (DTS).

§ 130.20 AO Technology Office

DTS has assigned the following authorities and responsibilities to the Chief of its AO Technology Office (AOTO):

(a) to develop, manage, and implement policy for AOTO IT personal property and resources, including other IT resources within the AOTO system boundary;

(b) to manage, operate, and inventory AOTO IT personal property and resources; and

(c) to develop, manage, and implement information security policy for the AOTO system boundary.

§ 130.30 AOTO IT Operations Security Officer

The AOTO IT Operations Security Officer is responsible for implementing and overseeing information security policies and requirements for the AOTO system boundary.

AO MANUAL

Volume 9: Information Technology

Chapter 2: IT Equipment Responsibility and Use

§ 210 General

This chapter establishes policy regarding responsibility for, and appropriate use of, government office IT equipment and services, including but not limited to:

- personal computers, related equipment, servers, and software;
- photocopiers, scanners, and facsimile machines;
- internet, intranet, and email service;
- wireless/portable technology;
- audio/visual equipment; and
- telephone equipment, services, and systems.

§ 220 Appropriate Use of IT Equipment

(a) Overview

(1) AO employees may use government equipment and services for officially authorized purposes, with some limited personal use of such equipment and services under the conditions set forth below.

(2) This policy provides users with a professional and supportive work environment while meeting expectations that federal tax dollars are spent wisely.

(3) The AO recognizes that users are responsible individuals, capable of balancing the privilege of limited personal use with the expectations of the American taxpayers and AO management that government resources are used appropriately.

(b) Personal Use Exception

(1) Employees are permitted limited personal use of government office equipment and services provided that the use:

(A) does not interfere with official business;

(B) occurs only during non-work time (i.e., when the employee is not otherwise expected to be addressing official business);

(C) involves minimal additional expense to the government; and

(D) is not illegal, disruptive, offensive, or otherwise inappropriate, as described below.

(2) Minimal additional expense occurs when the federal government already provides equipment and services, and the personal use results in:

(A) no additional charges,

(B) minimal wear and tear,

(C) limited use of consumables (e.g., electricity, ink, toner, paper, and/or supplies), and

(D) no more than minimal burdens on communications infrastructure and data storage capacity.

(3) This privilege may be revoked or limited at any time and does not convey to employees an inherent right to use government property for personal purposes. It also does not permit modifying equipment, including loading personal software or making configuration changes. Supervisors may further restrict personal use based on the needs of the office.

(c) Inappropriate Personal Use

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government equipment and services for inappropriate activities, including those that:

(1) are illegal, offensive, or harassing to co-workers or the public, such as hate speech, or material that ridicules others on the basis of race, color, religion, sex, national origin, or disability;

(2) could cause congestion, delay, or disruption of service to any government system or technology (including video, sound, and other large file attachments and mass mailings);

(3) involve any illegal activity (e.g., gambling, copyright violations);

(4) involve obscene, pornographic, sexually explicit, or sexually oriented material;

(5) are for commercial purposes or in support of outside business or employment activity of the employee or a friend or relative; or

(6) involve fund-raising, endorsements of products or services, lobbying, or any prohibited political activity.

§ 220.10 Responsibilities

(a) Users

(1) Review and adhere to all applicable rules, regulations, and standards of employment responsibility and ethical conduct. **See:** AO Code of Conduct (Legacy AO Manual, Vol. 2, Ch. 1, § 110).

(2) Practice good judgment when accessing and using any government equipment and/or services;

(3) Ensure that:

(A) any use of government property is for official business or is otherwise authorized and does not involve inappropriate activity;

(B) communications reflect appropriate business ethics and practices; and

(C) any personal use does not convey the appearance that the user is acting in an official capacity.

(b) Supervisors

(1) ensure that users are fully informed of usage policies;

(2) ensure that appropriate approvals are obtained when procuring IT equipment, access and resources; and

(3) observe the use of IT equipment, informing higher level management of suspected misuse.

§ 220.20 Privacy

(a) Authorized users should expect **no** privacy in the use of government equipment and/or services.

(b) No use of government equipment or services is entirely secure, private, or anonymous. Almost any use may be monitored or recorded.

(c) Users accessing and using government electronic equipment and services, including personal computers, mobile devices, network drives, email, internet and intranet service, expressly consent to monitoring of their usage and to access by appropriate officials to records created, received, or maintained by them.

(d) Users should be aware that internet sites capture the domain name of accounts accessing a specific site and maintain a record of the domain name. It could be embarrassing to a user and the judiciary if the domain name "uscourts.gov" were found on the access records of an inappropriate site.

§ 220.30 Penalties for Misuse

Users may be subject to penalties for inappropriate or unauthorized use of government office equipment and/or services. Depending on the nature and severity of the misuse, penalties may include administrative action ranging from counseling to removal from employment, criminal penalties, and financial liability. **See:** Legacy AO Manual, Vol. 2, Appx. F (Corrective Actions for Employee Misconduct).

§ 230 Wireless and Portable Technology

This guidance is for issuing and using wireless and portable equipment at the TMFJB and COSC, including:

- cellphones and smartphones;
- portable electronic devices (tablets, walkie-talkies, laptop computers);
- wireless access cards linking to an internet service provider (ISP); and
- other similar equipment that users use to conduct official government business.

§ 230.10 Issuance of Wireless Equipment

(a) Managers must justify requests for AO mobile and portable equipment for their staff, and justifications must show that the equipment is essential to support or conduct official business. The assignment of equipment may be on a permanent or temporary basis. Acceptable justifications include:

(1) supporting a critical system or program after hours,

(2) traveling to a court location more than once a month to conduct an audit or program review, or

(3) teleworking.

(b) Continuity of Operations

(1) Another important reason for issuing wireless and/or portable technology equipment is to maintain mission critical business during emergencies; as detailed in the AO Continuity of Operations Plan and Occupant Emergency Plan.

(2) The agency may issue, and require positions identified in the COOP and OEP to use, wireless and/or portable technology equipment to support AO operations.

(c) All requests are dependent on the availability of funding.

§ 230.20 Responsibilities

(a) Supervisor and AO Office Chief Levels

(1) Establish procedures to approve employees' equipment requests.

(2) Review and approve internal Form (IF) 407s (Request for Wireless and/or Portable Equipment) and submit the requests to AOTO for a technical review. Requests that don't provide adequate justification in terms of essential mission support should be disapproved.

(b) Users

(1) Contact AOTO to determine the most appropriate technologies to meet their needs.

(2) Complete IF 407 and sign the Requestor's Certification block.

(3) Use wireless and/or portable technology equipment consistent with § 220 (Appropriate Use of IT Equipment).

(4) Return equipment that is no longer required due to changing responsibilities or work assignments.

(c) AO Technology Office

(1) Oversees wireless and portable technology equipment utilization by the AO for TMFJB and COSC locations.

(2) Helps requesting offices select the appropriate wireless and/or portable technologies; if applicable, conduct compatibility testing and product licensing.

(3) Procures equipment and associated maintenance agreements.

(4) Maintains a current inventory of AOTO-managed, agency-owned wireless and/or portable technology equipment consistent with inventory management guidance. **See:** Redesigned AO Manual, Vol. 8 (Facilities and Security), Ch. 4 (Official Government Property), § 460.20 (Inventory). (**Note:** AOTO only manages AO equipment at the TMFJB and COSC.)

(5) As requested, provides mobile cost report to AO Office Chiefs.

(6) Provides AO help desk support for approved wireless and/or portable technology equipment.

(7) Conducts an annual assessment to determine if users still need the wireless and/or portable technology equipment issued to them.

§ 240 Telephones

This guidance is for using the telephone system at TMFJB and COSC.

§ 240.10 Telephone System

(a) All AO telephone system lines, including those used for fax machines and modems, are assigned one of three classes of service (COS):

(1) Restricted Access

Permits calls to any device on the National Internet Protocol Telephony (NIPT) system and 911 calls.

(2) Local Access

Permits calls within the DC Area.

(3) Standard Access

Permits calls within the United States and its territories, and Canada, Bermuda, and many Caribbean nations. Calls to other locations are not permitted.

(b) COS assignments are made based on the users' business requirements.

§ 240.20 Responsibilities

(a) AO Office Chiefs and Executive Officers

(1) Oversee the work of users to ensure that they adhere to § 220 (Appropriate Use of IT Equipment).

(2) Assign, revoke, or further restrict telephone access privileges at any time.

(3) As needed, request telephone usage reports from AOTO.

(4) Respond to periodic requests for updated user authorizations.

(b) Users

(1) Adhere to § 220 (Appropriate Use of IT Equipment), and

(2) Comply with the AO Code of Conduct (Legacy AO Manual, Vol. 2, Ch. 1, § 110).

(c) AO Technology Office

(1) Provide access to telephone services, monitor the use of those services, and take appropriate administrative action to assure quality and to deter misuse.

(2) When requested, process requests for telephone usage reports from AO Office Chiefs.

(3) Assign numbers to all managed telephones, fax machines, modems, etc. that are connected to the telephone system at TMFJB and COSC.

§ 250 Videoconferencing

This guidance is for the use of videoconferencing equipment at TMFJB and COSC.

§ 250.10 Videoconferencing Services and Facilities

(a) The AO provides videoconferencing services and facilities for use by AO offices and judiciary units.

(b) Depending on the purpose, size, and type of videoconference, different videoconferencing configurations may be required. For more information on scheduling a videoconference, contact the AO Help Desk.

§ 250.20 Responsibilities

(a) AO Technology Office

(1) Providing assistance and support to any office desiring to use videoconferencing services available via the AOWeb online conference room scheduler.

(2) Coordinating technical arrangements with remote locations. The integrated videoconference system(s) may only be used for authorized purposes by authorized videoconference specialists.

(b) Host

(**Note:** The term “host” includes the senior official of the office requesting the videoconference and/or the event’s designated point-of-contact.)

(1) Planning for a videoconference well ahead of the event. To ensure that all essential elements are in place at the right time, questions should be emailed to the AO Help Desk.

(2) Accountability for any misuse of videoconferencing resources.

(3) Recording the event. The host is responsible for including any recording requirements in the AOWeb online conference room scheduler meeting request.

§ 250.30 Procedures

(a) Planning

The host must:

(1) Coordinate the desired date and time with the remote site(s);

(2) Provide the names of all participants and their locations;

(3) Provide any applicable telephone numbers for the remote site locations; and

(4) Determine which support requirements (e.g., recording), if any, will be required.

(b) Reserving Videoconferencing Services

(1) As soon as the decision is made to conduct a videoconference (ideally, five work days prior to the desired date of the event), the host should email the AO Help Desk with the following information:

(A) confirm support requirements and technical arrangements sufficiently in advance of the event, and

(B) discuss the capabilities of each videoconference facility and help identify the one best suited to the host's needs.

(2) The host must remember that reserving a conference room via the AOWeb online conference room scheduler or directly with the office responsible for managing the room does not guarantee AOTO videoconferencing services. AOTO is responsible for providing such services **only** for events scheduled with the AO Help Desk.

(c) Cancellation

In the event the videoconference is canceled, the host must notify the AO Help Desk and the remote site participants as soon as possible.

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

AO MANUAL

Volume 9: Information Technology

Chapter 3: IT Security

§ 310 General

This chapter contains IT security policies for AO systems.

§ 320 Password Requirements

§ 320.10 General

(a) Passwords are an important component of computer security and a key means of protecting valuable AO information. A poorly chosen password may compromise the availability or integrity of AO system resources and data. Therefore, all users are responsible for taking the appropriate steps, described in this section, to select and secure strong, unique passwords.

(b) Password requirements are established as a means to protect the user, the data, and the integrity of the configuration of the systems. Network applications and systems managers/administrators must ensure that these password requirements are in place and enforced for the systems or networks they manage, or request an exception to the policy on Internal Form 413 (Request for Exception to Security Policy).

(c) User-level passwords must adhere to the following rules:

(1) Passwords must be changed on at least a semiannual basis.

(2) Passwords must be at least 8 characters in length.

(3) Passwords must contain a combination of upper and lower case alphabetic characters.

(4) Passwords must contain at least one digit or special character (e.g., !, @, #, $, %, &, *, +).

(5) Passwords should not be shared with anyone, including administrative assistants, secretaries or supervisors. All passwords are to be treated as sensitive, confidential AO information.

(6) Passwords should not be stored in a file on any computer system (including mobile devices) without encryption. (**Note:** Encryption is the processing and altering of data so that only intended recipients can access it. The recipient must have the proper decryption key and program to decrypt the data back to its original form.)

(7) A system administrator may not use the same password to gain root access to two different servers. To be in compliance with this rule, users must ensure a unique password for any system to which they have logon access.

(d) System-level passwords (i.e., root, or individuals with full system administrator privileges on a network or application system) must adhere to the following rules:

(1) Passwords must be changed at least on a quarterly basis.

(2) Passwords must be a minimum of at least 9 characters in length.

(3) Passwords must contain a combination of upper and lower case alphabetic characters.

(4) Passwords must contain at least one digit or special character (e.g., !, @, #, $, %, &, *, +).

(5) Users with logon accounts that have system administrator, root or full access privileges must ensure a unique password for all systems to which they have logon access.

(6) Passwords should not be stored in a file on any computer system (including mobile devices) without encryption.

(7) System level passwords (i.e., root, system administrator) must be stored in a locked file cabinet in a secure area for the purpose of system recovery/system maintenance in the event the person normally performing these functions is absent or unavailable. Only those individuals designated and authorized by an AO senior staff member will be granted access to these secured files.

(e) User Responsibilities

Users are responsible for ensuring that all passwords they create and/or use that grant access to any AO system or network comply with this policy. Passwords not meeting these criteria must be changed.

(1) For staff whose worksite is the Thurgood Marshall Federal Judiciary Building (TMFJB) and Court Operations Center (COSC), exceptions to this policy require the concurrence of the Technical Review Team. Request should be submitted to the AO Help Desk on Internal Form 413 (Request for Exception to Security Policy).

(2) Staff at other locations should use an exception request form appropriate for the location. **See:** Guide, Vol. 15, § 380 (Security Policy Exceptions).

(f) Supervisor Responsibilities

Supervisors are responsible for ensuring that all users under their direct supervision are made aware of this policy.

(g) Other Responsibilities

(1) AO system and/or network managers/administrators with oversight and maintenance responsibility for user account configuration and maintenance must configure servers and applications to require users to change their passwords at least semiannually.

(2) System managers, network managers, and system administrators will employ the use of strong password tools or administrative settings on all applicable servers to ensure passwords granting system or network access meet the criteria outlined in this chapter.

(3) If specific accounts cannot be brought into compliance with this policy due to configuration limitations or other compelling reasons, the relevant AO Office Chief must complete and send Internal Form 413 (Request for Exception to Security Policy) to their respective Associate Director, the ISO for the system, ITSO, and AOTO.

(h) Penalties for Non-Compliance

Any user or system owner found to be in violation of this policy may be subject to loss of account privileges until such time as compliance is met. Anyone found to create or alter any password configuration contrary to this policy may face performance and/or disciplinary action. For detailed information on performance, conduct, and disciplinary standards, **see:** Redesigned AO Manual, Vol. 4, Ch. 1 and Ch. 7.

§ 320.20 Additional Guidelines for Password Construction

The following guidelines are provided to help users in choosing appropriate passwords.

(a) **Good, strong passwords** have all of the following characteristics:

(1) Contain both upper and lower case letters (i.e., a-z, A-Z).

(2) Contain numbers and/or punctuation (e.g., 0-9, !@#$%^&*()_+).

(3) Are at least eight alphanumeric characters long.

(4) Do not form a word in any language, slang, dialect, jargon, etc.

(5) Are not based on personal information, names of family, etc.

(6) Are easy for you to remember, since they should not be written down or stored online.

Note: A strong password can be formed from a familiar song title, phrase, or sentence. For example, choose “ibaHdn7” or "Iba3hdn” as a password based on the song title, "It's Been A Hard Day's Night”; or "mnpiE2r" or "1mnPietr" based on the phrase, "My new password is easy to remember." ***Do not use any of these examples as actual passwords*****.**

(b) **Poor, weak** passwords have the following characteristics:

(1) Contains less than eight characters;

(2) Are words found in a dictionary; or

(3) Are common usage words such as:

(A) names of family pets, friends, co-workers, or famous people;

(B) computer terms and names, commands, sites, companies, hardware, software;

(C) personal data (e.g., birthday, address, phone number);

(D) alphanumeric patterns (e.g., aaabbb, zyxwvuts, 123456);

(E) any of the above spelled backwards; or

(F) any of the above preceded or followed by a digit.

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

AO MANUAL

Volume 9: Information Technology

Chapter 4: Protecting Sensitive Information

§ 410 General

This chapter establishes the AO policy for proper handling of sensitive information by the AO workforce including volunteers, interns, and detailees. The policy is intended to heighten awareness of the risk of harm to individuals, the U.S. government, and private organizations if that information is misused, and to mandate precautions to ensure its protection and appropriate use.

§ 420 Proper Handling of Sensitive Information

(a) Mishandling of sensitive information can result in harm to individuals, the U.S. government, and private organizations if that information is misused.

(b) AO workforce members should be aware of how to handle sensitive information and must follow the mandatory precautions set forth below to ensure that sensitive information is protected and appropriately handled.

§ 420.10 Definitions	
AO Workforce user	Someone entrusted to have access to an AO system or is responsible for a user account (or accounts) on automated systems within the AO.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

§ 420.10 Definitions	
Media	Physical objects on which data are stored, including but not limited to electronic storage media (e.g., hard drives, thumb drives) and paper.
Mobile Device	Handheld or other portable computing equipment with an operating system.
Sanitization	Expungement of electronic media to make access to or recovery of data or other information impossible. Most common types of sanitization: destruction (e.g., smashing), purge (i.e., software and hardware data removal), and data overwriting. **See:** Guide, Vol. 15, § 550.30 (Securing Information).
Sensitive Information	Any data or other information for which public disclosure, or disclosure to users who do not have a need to know in order to perform their jobs, can harm individuals, the U.S. government, and private organizations. Information may be considered more or less sensitive (or not sensitive at all) depending on the context in which it is stored, presented, or used. **Examples:** • *Personal* – Social Security numbers, dates of birth, financial account numbers, medical information, names of minor children, judges addresses, certain information on personnel actions, performance plans, and appraisals. • *Financial* – Bank, credit card, and certain payroll information. • *Procurement* – Content and evaluations of technical/cost proposals. • *Proprietary* – Information in which an individual or organization has a legitimate property right or other valid economic interest that could be compromised through unauthorized disclosure or other use. • *Court-related* – Sealed cases, sealed documents, or information relating to the safety or security of court personnel or facilities. • *Privileged/confidential* – Information protected through recognized confidential relationships (e.g., attorney-client privilege). • *IT* – User accounts, passwords, network diagrams, system security. • *Official business* – Proposed budgets, draft plans or policies, other information intended solely for the consideration of internal decision makers or other confidential audiences.

§ 420.20 Protective Measures

(a) All AO workforce users (**see:** AO Manual, Vol. 9, § 120):

(1) Must be vigilant stewards of the sensitive information placed in their custody or used by them in the course of their job duties.

(2) Complete annual training on the appropriate use and handling of sensitive information as part of the AO's IT security training and awareness program.

(b) Sensitive information:

(1) Must be maintained and handled securely (e.g., encrypted, password protected, or in a secure location).

(2) Normally should not be stored on a mobile device or in portable electronic media. If a waiver is granted for this purpose by the relevant supervisor or other person designated in a particular department, an individual with an operational or other business need may be authorized to store sensitive information on a mobile device or in portable electronic media so long as he or she does so using a secure format approved by AOTO. Additional guidance can be found on JNet under Mobile Devices Need Security Too.

(3) Must be handled with awareness of the surroundings so that it is not inadvertently disclosed to unauthorized individuals. For example, sensitive information must not be:

(A) Discussed in areas where the discussion might be overheard by unauthorized individuals.

(B) Left in plain sight when an authorized user is not present or when any unauthorized individual is present.

(4) Must be labeled as such and accompanied by any special handling instructions that may be needed. For example, a paper document must have a cover page identifying its contents as sensitive.

(5) Must be secured (e.g., in a locked drawer, cabinet, or safe, or with a password-protected computer screen saver) when unattended or not in use.

(6) Must be double-sealed, with the inside envelope appropriately labeled as containing sensitive information, if transported through the mail or by a courier/messenger service. Also, the receipt and delivery of the media must be monitored and accounted for to ensure that the sensitive information is neither lost nor potentially compromised while in transit.

(7) Must be retrieved promptly from a printer or copier (including the original and all copies) whenever it is printed or duplicated.

(8) If faxed, it must be retrieved promptly from the sending machine, and the recipient alerted to retrieve the copy from the receiving machine. When a document containing sensitive information is expected to be faxed, the receiving machine should be watched

closely and the copy retrieved as soon as it arrives. When available, a fax machine located in a secure room must be used at each end of the process.

(c) When no longer needed and before being donated or otherwise disposed of, AO-owned or managed computer equipment or electronic media containing sensitive information must be brought to the local help desk for sanitization, or otherwise sanitized through an AOTO-approved method.

(d) When no longer needed, paper media containing sensitive information must be disposed of in a secure disposal bin or paper shredder.

(e) A user may access sensitive information in a system, application, or record only for business purposes as authorized by relevant management.

(f) Any actual or suspected loss or improper use of sensitive information:

(1) Must be promptly reported as provided in the *Sensitive Information Incident Response Procedures* ("Incident Response Procedures").

(2) Must be addressed, once it is reported, by the local Information Technology Security Officer and other appropriate personnel (e.g., AO Security Team) according to the *Incident Response Procedures*.

(3) Must be reported by the AO Security Team to the AO Deputy Director as provided in the *Incident Response Procedures*.

§ 420.30 Responsibilities

(a) All members of the AO workforce with access to sensitive information are responsible for complying with this policy, and with any rules of behavior, requirements or guidance provided by other applicable policies. No individual will be afforded access to any IT system or application containing sensitive information until he or she has been informed of and acknowledges these policies.

(b) Supervisors must ensure that access to sensitive information is limited to those with a business need for such access, and for promoting compliance with this policy by the individuals who report to them.

(c) Program offices and/or system owners are responsible for the successful operation of information systems within their program areas and are accountable for implementing reasonable and effective security safeguards (or controls) to protect the security and privacy of information assets within their purview. Successful operation is facilitated by adhering to the *Information Technology Project Management Process (ITPM)*, which includes the creation of a Systems Security Plan (SSP) during the project planning phase.

(1) The SSP provides an overview of the security requirements for the information system and describes the safeguards in place or planned for implementation to provide a level of security appropriate for the information processed. Occasionally, a system takes advantage of another system's security safeguards (i.e., leverages the physical controls of an existing data center or uses the authentication features of another application (e.g., JENIE)). These safeguards are considered to be inherited and noted as such in the SSP.

(2) Before operational deployment and at regular intervals after that, program offices and/or system owners must test their security safeguards (as documented in their SSP) to ensure the information system is adequately secured throughout its life cycle. As the system evolves over time, the SSP should be updated to reflect the system’s functionality and security profile. At a minimum, the SSP must be reviewed for ongoing accuracy whenever a major system change occurs or at least every two years, whichever is soonest, and submitted through the ITPM process for an independent review by the Information Technology Security Office (ITSO).

§ 420.40 Issue Resolution

(a) Questions concerning proper handling of sensitive data should be directed to the AO Help Desk or AOTO’s IT Operations Security Officer.

(b) Questions concerning the sensitivity of specific data or the responsibility for protecting sensitive information in a given context should be directed to the relevant supervisor, or to the AOTO Information Technology Security Officer, who will coordinate with appropriate AO authorities on a response.

§ 420.50 Enforcement

Violations of this policy may result in loss of information technology resources or limitations of the use of those resources, and appropriate disciplinary action.

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

AO MANUAL

Volume 9: Information Technology

Chapter 5: Network and Internet Access

---

§ 510 General

This chapter provides the policy for requesting and authorizing network and internet access to the AO's Local Area Network (LAN) at the Thurgood Marshall Federal Judiciary Building (TMFJB) and the Court Operations Support Center (COSC).

§ 520 Network Access

(a) Network access is limited to AO authorized employees, contractors, and interns (collectively referred to as the *AO workforce*) who require access to the AO LAN based on official duties and may be revoked at any time.

(b) Network access is limited to judiciary information and software programs specifically necessary for the user to conduct official duties.

§ 520.10 Responsibilities

(a) AO Supervisors

(1) Obtain network access for new staff by using Internal Form (IF) 403 (IT Service Request).

(2) Notify the AO Help Desk by email when circumstances arise that require modifying or deactivating an employee's AO network access, such as a user's transfer within the AO or a change in

responsibilities. When an employee separates from the AO, AO remote access deactivation is part of the mandatory clearance process.

(b) Contracting Officer Representative (COR)

CORs are responsible for notifying AOTO via an InfoWeb Contractor Status Change Notification or email to the AO Help Desk when there are circumstances that require a contractor's AO network access to be modified or deactivated, including when a contractor has completed his/her contract assignment or a contractor’s assignment has changed.

(c) AO Network User

Read, understand, and adhere to the:

(1) Redesigned AO Manual, Vol. 9, § 220 (Appropriate Use of IT Equipment);

(2) Legacy AO Manual, Vol. 2, Ch. 1, §110 (Code of Conduct), and

(3) The applicable policy in this volume.

(d) AO Technology Office (AOTO)

(1) Process IF 403s

(2) Notify users when technical arrangements are made and provide appropriate account information.

(3) Deactivate a user’s AO network account upon official notification as appropriate.

§ 530 Remote Network Access

(a) Remote network access is the ability to access the AOLAN through the internet from a remote location; access is granted based on official responsibilities and may be revoked anytime.

(b) Remote network access is limited to the authorized workforce members that require access to the AO LAN.

(c) Remote network access is limited to judiciary information and software programs specifically necessary to meet user responsibilities.

(d) Before remote network access may be authorized, users must address the security conditions listed below in § 530.10(d)(6).

(e) Approval of an employee's request for remote network access does not imply approval of a work-at-home or telework agreement.

(f) For information on participating in the agency's Telework Program, **see:** Legacy AO Manual, Vol. 2 (Human Resources), § 520 (Telework).

§ 530.10 Responsibilities

(a) Office Chief or Division Chief

Approve or disapprove requests for remote network access.

(b) AO Supervisor

(1) Approve IF 401 (Remote Access Request) as documentation that the requestor requires remote network access for official responsibilities and specifies a need for access to certain computer programs, systems, and information requested.

(2) Ensure that AOTO is notified via an email to the AO Help Desk when there are circumstances that require an employee's AO network access to be modified or deactivated, including a user's transfer within the AO or change in responsibilities. When an employee separates from the AO, AO remote access deactivation is part of the mandatory clearance process.

(3) If needed, a supervisor may request customized reports of AO remote network access usage anytime by contacting AOTO.

(c) Contracting Officer Representative (COR)

CORs are responsible for notifying AOTO via an InfoWeb Contractor Status Change Notification or email to the AO Help Desk when there are circumstances that require a contractor's AO remote network access to be modified or deactivated, including when a contractor has completed his/her contract assignment with the AO.

(d) AO Remote Network Access User

(1) Read, understand, and adhere to Redesigned AO Manual, Vol. 9, § 220 (Appropriate Use of IT Equipment) and the policies in this volume.

(2) Complete an IF 401, obtain the appropriate approvals, and submit the approved form to AOTO for processing. The justification block on the form must state:

(A) why AO remote network access is necessary to fulfill responsibilities;

(B) how security considerations will be met at the remote site.

(3) Ensure that any special needs or requirements are communicated to AOTO.

(4) Verify that the remote site provides the necessary level of security and protection for the government and property and/or confidentiality of data.

(5) For non-AO computers, install the software AOTO provides and make security arrangements at the remote site according to these guidelines and the terms listed on the IF 401.

(6) By signing the IF 401, the user agrees to adhere to the following mandatory conditions (also listed in the IF 401):

(A) All security policies for use in the AO office environment must also be observed when using or connecting to AO resources while at the remote location.

(B) A password-protected screen saver that automatically activates after no more than 30 minutes of inactivity and can be invoked on demand must be used.

(C) AO sensitive information must be maintained and handled securely to protect it from unauthorized disclosure (e.g., encrypted, password protected, or stored in a secure location) in accordance with Redesigned AO Manual, Vol. 9, Ch. 4 (Protecting Sensitive Information).

(D) AO sensitive information is not to be stored on any non-AO computers;

(E) When no longer needed, paper media containing sensitive information must be immediately disposed of in a secure disposal bin or paper shredder;

(F) AO users may not change operating system configurations, install new software, alter equipment or add to it in any way (e.g., expanded memory, wireless cards), or download software from systems outside of the AO onto AOTO managed computers unless authorized to do so (i.e., Local System Administrators);

(G) Any non-AO computers used to connect to the AO's information resources must use an approved antivirus program installed and configured with the latest updates. In addition, users must ensure that all security patches are applied as soon as possible;

(H) Use firewall technology if a continuous connection exists while connected to AO information resources (e.g., cable or digital subscriber line (DSL) modem);

(I) Configure wireless routers to ensure maximum security;

(J) Use a surge protector at the remote location; and

(K) Notify your immediate supervisor, when the need for remote network access no longer exists and return all AOTO issued computer software to AOTO.

(e) AOTO

(1) Process IF 401s.

(2) Coordinate with other offices in the Department of Technology Services (DTS) on contractor remote access requests.

(3) Notify the user when technical arrangements are made and provide appropriate account information.

(4) Change or deactivate the AO remote network access upon official notification.

(5) Upon request, prepare customized AO remote network access usage reports upon request from AO Office Chiefs.

§ 540 Internet Access

(a) Internet use is constrained to help ensure security and appropriate use by blocking access to sites that might be deemed as inappropriate for the AO workforce to access from the AO’s IP addresses.

(b) Users may request that specific sites be unblocked for official business purposes; however, unblocking a site opens that site to all users and thus requires forethought, sound business judgment and notification to the appropriate Office Chief or Executive Officer.

§ 540.10 Responsibilities

(a) AO Office Chiefs or Executive Officers may request monthly internet usage reports for their employees.

(b) AO users must:

(1) Adhere to:

(A) Redesigned AO Manual, Vol. 9, § 220 (Appropriate Use of IT Equipment);

(B) Legacy AO Manual, Vol. 2, Ch. 1, §110 (Code of Conduct); and

(C) the applicable policy in this volume.

(2) When appropriate, request that a site be unblocked by sending an email to the AO Help Desk that:

(A) provides a justification for unblocking the site, and

(B) includes the supervisor(s) and appropriate Senior Staff member in the addressee line of the email request.

(3) Notify their supervisor and the AO Help Desk by email when access to specific unblocked sites is no longer required.

(c) AOTO must:

(1) Provide access to internet services;

(2) Process authorized email requests for unblocked access to specific sites within one working day of receipt;

(3) Process requests for Internet Usage Reports from AO Office Chiefs; and

(4) Assign transmission control/Internet protocol (TCP/IP) addresses to all workstations connected to the TMFJB and COSC LAN.