United States District Court
Northern District of Illinois

Information Technology Policy

Rev. 7/25/2019

Table of Contents

Background/Purpose

This document is a comprehensive repository of all the required IT security policies required by the *Guide to Judiciary Policy (Guide)*. Each major section of this document corresponds to one of the 18 required policies from the *Guide*. Each section outlines the policy, procedure, and verification of each stage of the policy. These policies are intended to secure and protect all IT users, administrators, and equipment in the US District Court for the Northern District of Illinois. The security and protection of Court operations and information is tantamount to ensuring efficient, accurate, and excellent service to the citizens of the United States of America and visitors who appear in our Court.

Points of Contact

For further information on IT security policies or procedures, please contact:

Thomas Bruton
Clerk of Court
(312) 435-6860

Minesh Thakkar
Systems Manager
(312) 435-5664

1. Appropriate Use of IT Systems

1.1 Introduction

When performing official duties, there are important restrictions to be aware of when using any court IT system. These restrictions are in place to uphold the confidentiality, integrity, and availability of all Court IT systems and information. These provisions must be followed because they protect not only one's official data, but also all electronic records and systems at the Court. This document will outline what is considered appropriate use of Court IT systems as well as provide some examples of what is and is not allowed. By following these requirements, Court operations will continue safely and securely.

1.2 Scope

This policy applies to all users and administrators of ILND Court IT equipment and services.

1.3 Policy

1.3.1 General Provisions

1. IT equipment and services are primarily for official government business only.

2. Judiciary employees are allowed limited personal usage subject to the following provisions:
   a. Usage may not interfere with official business.
   b. It may not add additional cost to the government.
   c. Personal usage may only occur during non-work time.
   d. The Chief Judge or Clerk of Court may revoke personal usage at any time.
   e. Personal usage may not violate the Code of Conduct in any way.
   f. It may not circumvent any security protocol or policy in place.

3. Users are not allowed to install any software on any government IT device without appropriate permission from the Systems Manager or the Information Technology Security Officer (ITSO).

4. Non-government owned software is not allowed on any government owned device with the exception of judges' devices.

5. All copyrighted music and personal files owned by a user are not allowed on any government device. Only files created, purchased, and used in the performance of official government work are allowed due to copyright regulations.

6. Users are not allowed to access systems and services that they are not authorized to use.

7. No user will allow any non-court personnel to access government equipment and services at any time.

8. No user will disclose any internal or confidential government data without authorization.

9. Any additional requirements present in the *Guide* Volume 15 Ch. 3, but not mentioned here, are included in this policy and shall be enforced as appropriate.

1.3.2 Email and Instant Messaging

1. Email is provided solely for official government operations.

2. At no time, is email to be used for any personal financial business
    a. This includes signing up for personal newsletters, coupons, or any other services not used for official government work.
    b. It may also not be used in a manner that uses the position of the user to further private gain. It is strictly for public official use as per Canon 2 of the Code of Conduct.
    c. The only exception is when sending a personal email that contains a disclaimer you are not acting in an official capacity, but this action should be limited.

3. Users are responsible for keeping a clean mailbox. Email that is no longer needed for any reason should be deleted to save space on the mail server as the email server is a shared resource.

4. Instant messaging may only be conducted using the AO approved IM software and is only for official government business.

1.3.3 Court Supplied Software

1. All software provided on government devices is primarily for official business only.

2. Government owned and licensed software may not be used for conducting private commercial business at any time.

3. All legal research tools and CM/ECF are provided solely for official government business. Users may not perform personal searches about any case or person at any time that is outside the scope of official work.

4. Government software is not to be installed on personal machines without authorization of the Systems Manager or judiciary licensing policy.

1.3.4 Wired and Wireless Network

1. The network is provided primarily for official government business.

2. At no time may a user intentionally perform any function that will interfere, disrupt, or disable the network.

3. Streaming services used for a personal nature are not allowed on the network.
    a. This includes Netflix, Pandora, Spotify, or any other streaming website.

4. Streaming services may be used if they are used for official Court business only.
    a. This includes career training, evidence examples, or any other need that falls under official government business.

1.3.5 Court Supplied Devices

1. Court supplied devices, including but not limited to desktops, laptops, cell phones, and other issued devices are intended primarily for government usage only.
    a. These devices are subject to the personal usage guidelines listed.

2. At no time is any non-court employee allowed to access or use a court-supplied device.
    a. Contractors with the proper permission are authorized to access court devices.

3. All tech support for such devices shall only be provided by the USDC Systems Department or the AO Support Office.

4. At no time is any Court supplied mobile device to be used or given to any non-court personnel for any reason.

1.4 Procedure

To ensure that all employees are aware of this policy, it shall be posted on an internal web page and copies may be received by request from Human Resources or the Systems Department. All newly hired employees shall receive a copy of this policy as part of their new hire orientation. All employees agree to be bound by this policy as a condition of using all court IT equipment and services at all times. If non-compliance is identified for Clerk's Office staff, the Clerk of Court will be notified. For chambers staff, the appropriate judge will be notified. Any changes made to this policy shall be communicated to all court employees and contractors hired by the court when they are approved for distribution. This policy will be reviewed annually by the Systems Department Security Team and updated as needed to maintain compliance with the appropriate federal laws and/or Judicial Conference policies.

1.5 Verification

To verify compliance, inspections of Court IT systems and services will be performed to ensure normal systems operations. In the case of remote monitoring and inspections services, monitoring shall occur at least on a monthly basis. When devices are received and maintained by the Systems Department staff, they shall be checked for compliance with judicial access policy. The Systems Department is responsible for monitoring compliance of these provisions and communicating violations to the appropriate authority. The following list shows some, but not all, of the methods that compliance may be verified:

1. Routine network monitoring

2. Routine inspection of devices as technicians perform maintenance

3. Routine monitoring using remote system management and monitoring software

4. Notification of violations from the AO Security Operations Center, Network Management Facility (NMF), or Systems Deployment and Support Office (SDSO).

5. Any notifications from automated security and monitoring systems in place

2. Configuration Management

2.1 Introduction

Configuration management is a necessary part of IT operations that minimizes duplication of work. It also ensures a base standard for all configured IT systems from a security and management perspective. This increases efficiency of operations and minimizes operational deployment time. Configuration management also allows auditing and tracking of changes that ensures ease of troubleshooting when issues arise through normal operations.

2.2 Scope

This Secure Configurations for Hardware and Software policy applies to each of the organization's workforce members who have contact or potentially may have contact with the organization's data, applications, and computing resources. This includes, but is not limited to employees, contractors, vendors, service providers, volunteers, or any others who have or may come into contact with the organization's data, whether in a paid or unpaid capacity. Exceptions to this policy must be properly approved and documented in accordance with the organization's control exception policy.

2.3 Policy

IT Administrators must establish and actively manage secure hardware and software baseline configuration images, conduct strict change management procedures, and remotely manage only over secure channels. IT Administrators will establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The ITSO is responsible for ensuring baseline configurations are created for all networking equipment that ensures a secure networking environment. All network equipment will be properly secured so that only authorized personnel are able to access the management and administration functions of the equipment.

2.4 Procedure

1. The US District Court for the Northern District of Illinois will establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system and will incorporate any applicable Judicial Conference policies for security and management. These images should be validated and refreshed on a regular basis to update their security configuration.

2. The Court Unit will follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Prior to operational deployment, all systems, hardware, and software configurations must be documented. The documentation will describe the following:
    a. What configuration was needed

b. How the configuration was implemented
c. Technician(s) responsible for managing the system

All deployment processes will be documented and will describe the following:

a. Method and instructions for deployment
b. Users or groups deployed to
c. Technician(s) responsible for deployment

Documentation will be maintained for the lifecycle of the deployed system.

3. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization’s change management processes. Images should be created for workstations, servers, and other system types used by the organization.

2. In the planning stages of implementing new systems, Systems staff will document the required configuration needed for the system to fit this policy and operating requirements.

4. When developing and testing the method to deploy the system, the required documentation for deployment will be created once testing is complete.

5. After successful configuration and deployment, any further changes requested outside of the Systems Department must be requested via the appropriate change management form by a member of management. Once approved, the technicians assigned to the system will change the configuration and document the changes.

6. All remote connections to network equipment will have the data transmissions encrypted, if possible, to prevent interception of system administration information. The Court Unit will perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

7. Network staff will review the networking equipment configurations at least quarterly to ensure they are properly configured and secured.

2.5 Verification

1. The Systems manager is responsible for ensuring that Systems staff are properly generating documentation according to this policy.

2. All documentation regarding configurations will be kept in a centralized secure network share and organized appropriately to ensure Systems staff may quickly find the appropriate documents as needed.

3. Annually, all existing documentation will be reviewed by the Systems Manager to ensure the systems described are still deployed. If they are no longer in service, the documentation must be destroyed properly.

4. All change management requests must be reviewed by the technicians managing the system and approved by Systems Manager, if applicable.

3. Contingency Planning and Disaster Recovery

3.1 Introduction

IT systems are necessary for the normal operation of the court. These systems have varying levels of importance to the overall operations and therefore must have protections in place to ensure the recovery and return to normal operations in the event of a disaster and other contingencies. This policy establishes the procedures necessary to ensure IT staff can quickly restore operations after disruptions.

3.2 Scope

This policy applies to all USDC ILND IT equipment and staff.

3.3 Policy

The ILND Systems Manager and ITSO will develop a comprehensive approach for information system contingency planning. They will document procedures in information system contingency plans (ISCPs) ensuring the three recovery phases, activation/notification, recovery, and reconstitution are employed following system disruptions. The manager and ITSO will identify alternate storage and processing strategies and assign IT staff roles and responsibilities for implementing ISCP procedures.

1. Phase 1: Activation
    a. The degree of disruption is evaluated and communicated to the Chief Judge, Clerk of Court, ILND Systems Manager and ITSO.
    b. The estimated duration of outage is determined.
    c. Court personnel are notified of an outage if necessary.

2. Phase 2: Recovery
    a. The team responsible for the system will begin recovery operations.

3. Phase 3: Reconstitution
    a. The team will then test the system to ensure it has returned to normal operations.
    b. Cleanup tasks are performed.
    c. Court personnel are notified of the resolution.
    d. Documentation of the issue and a root cause analysis are created for future reference.

3.4 Procedure

1. If not documented in the COOP plan, then staff will categorize each IT system by its level of impact on operations if disrupted.
    a. Category 1: Critical
        i. These systems are mission critical to normal operations and if disrupted will cause loss of normal business operations.
    b. Category 2: Important
        i. These systems are important, but if disrupted will not disturb normal operations in the short term.

    c. Category 3: Desired
        i. These systems are desired, but if disrupted are not necessary to restore until critical or important systems are operational.

2. Once categorized, staff will document the following:
    a. Recovery Time Objective: The amount of time this system must be restored and tested as working within.
    b. Recovery Point Objective: The amount of time that data can be lost without disrupting business

3. Staff will then document what hardware, software, and equipment is needed to restore the system to normal operation.

4. Next, staff will document the order in which services and processes must be restored on the system to return it to normal operations.

5. Finally, staff will note who is responsible for each section of the plan's operations.

3.5 Verification

1. To ensure an ISCP is functional, IT staff will train for the plan and then test the plan in a simulated disaster at least annually.

2. The test will include a tabletop discussion that allows members of the team to understand and discuss their roles in a simulated event.

3. A functional exercise that simulates a live event where members of the team perform the steps of the plan at least when the DRP has been changed.

4. System owners and the ITSO will conduct an annual review of the ISCP plans to ensure they are up to date.

4. Incident Response

4.1 Introduction

The District Court for the Northern District of Illinois (ILND) is committed to providing a timely and comprehensive response to adverse events such as computer viruses, IT device theft, automated attacks, and intrusions.

4.2 Scope

This policy applies to all court IT personnel and approved contractors.

4.3 Policy

In preparation for timely and adequate response to information security incidents, the Systems Department will develop and maintain an Incident Response Plan that outlines the following:

1. The resources and staff assigned to plan and support incident response.
2. The responsibilities for each identified incident response role.
3. The designated members of the Computer Emergency Response Team (CERT).
4. Detailed instructions for implementing the court's incident response capability.
5. Describe reporting and tracking requirements.
6. Define reportable incidents and establish incident categories.
7. Define impact containment procedures.
8. Define evidence preservation and collection procedures.
9. Establish internal and external procedures for incident notification, including the facilitation of information sharing across the court regarding IT security vulnerabilities, threats, alerts, and incidents.
10. Describe how the court interfaces with external incident response support.
11. Define expectations of incident response performance, both internally and when interfacing with JASIRC.

4.4 Procedure

1. The court’s Computer Security, ITSO, and Systems Manager, contact information shall be updated when a designated person is changed.

2. Training shall be conducted annually for the Computer Emergency Response Team members in their responsibilities detailed in the IRP.

3. The IRP will be tested annually through a tabletop exercise involving the CERT and several non-CERT members.

4. Keep the plan secure and protected from unauthorized distribution.

5. Distribute the IRP to key incident response persons designated in the Incident Response Plan.

6. Update the IRP, as appropriate, to reflect changes in staff, procedures, and lessons learned from post-incident reviews.

7. Redistribute the Plan to key incident response personnel whenever it is updated.

4.5 Verification

1. Annually review and update the court’s “Computer Security,” “ITSO,” and “System Manager” contact information in InfoWeb.

2. The Systems Manager and ITSO shall review the IRP annually.

3. The results of the training exercises and annual testing shall be provided to the Clerk of Court and retained for auditing purposes until the next cycle.

5. Information System Access Control

5.1 Introduction

In order to ensure the best security, it is necessary to make sure that access controls are in place to prevent unauthorized access to systems. Systems must be secured to make certain only those trained or authorized to use them are able to and all others are denied access. It is also necessary to prevent intruders from accessing systems and potentially disrupting Court operations.

5.2 Scope

This Information System Access Control policy applies to each of the organization's workforce members who have contact or potentially may have contact with the organization's data, applications, and computing resources. Exceptions to this policy must be properly approved and documented in accordance with the organization's control exception policy.

5.3 Policy

1. The Systems Department is responsible for ensuring access controls are in place for all Court information systems.

2. The ITSO is responsible for creating a process to grant authorization to systems using the currently implemented account management systems.

3. Accounts are to be created and maintained using the rule of least privilege. This rule means that users will only be granted the minimal permissions possible to perform their tasks on the systems.

4. If possible, role based access control privileges will be used for ease of management.

5. Administrative accounts are to be used only for administrative functions and not day-to-day operations. Standard accounts must be used when not performing privileged actions.

6. IT Administrators must define, track and limit the use of Administrative Privileges.

7. All permission changes must be approved by a Manager or the Clerk of Court using the appropriate change request form. The Clerk of Court and the Chief Judge have the authority to deny any requested changes in the interest of security.

5.4 Procedure

1. System Access Controls will be maintained using the appropriate security systems. If possible, the access control system should be centralized to make it easier to manage.

2. The ITSO is responsible for ensuring all permissions are properly set so that no user is granted privileges they should not have. The US District Court for the Northern District of Illinois will minimize administrative privileges and only use administrative accounts when they are required;

will implement focused auditing on the use of administrative privileged functions and will monitor for anomalous behavior.

3. The ITSO may delegate administrative functions for creation of accounts, permissions, and other administrative functions to trained IT personnel.

4. All changes to a user's base permissions will be documented and provided upon request to the Clerk of Court.

5. The Court Unit will use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

6. Before deploying any new devices in a networked environment, The Court Unit will change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

7. The Court Unit will configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

8. The Court Unit will configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

9. The Court Unit will require that user accounts use long passwords on the system (longer than 14 characters).

10. Administrators should be required to access a system using a fully logged and non-administrative account.

11. Administrators will use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

5.5 Verification

1. The Internal Control Analyst will conduct an audit no less than annually of all access controls to ensure permissions are properly set and privileges are at the appropriate levels.

6. Information System Backup and Storage

6.1 Introduction

Digital information is one of the judiciary's most important assets, which grows in volume consistently year after year. With this growth comes the need to protect the confidentiality, integrity and availability of judiciary data with a comprehensive backup and storage strategy. Current and available backups are a lifeline when data is lost during emergency events. This section details the backup and storage policies for the court.

6.2 Scope

This policy applies to all Court IT systems that require backup and storage of data.

6.3 Policy

The ILND Systems Manager and ITSO ensure a comprehensive backup and storage program is developed and corresponding procedures identified and documented for its implementation. Backup and storage procedures include activities for data categorization, backup frequency and testing, data storage, and data restoration to ensure data is successfully recovered after disruptive events have occurred. The following categories and times will apply in this policy.

1. Category 1: Critical Data
    a. This data is vital to normal operations of the court. Loss of this data could severely cripple judiciary operations.
    b. Category 1 Recovery Time: Within one hour

2. Category 2: Important Data
    a. This data is important to normal operations concerning business plans and financial information.
    b. Category 2 Recovery Time: Within 1 or 2 business days

3. Category 3: Support Data
    a. This data supports the operations of the court but it is not needed for successful completion or primary tasks.
    b. Category 3 Recovery Time: Within 1 to 2 weeks

6.4 Procedure

1. Incremental system backups are performed every night.

2. Full system backups are performed once a week.

3. Incremental backups are kept on disk for four weeks.

4. Full backups are kept on disk for six weeks, and then transferred to tape for long-term storage.

5. Once a month, or when the tape library is full, tapes are removed from the tape backup server.

6. Tape backups are kept onsite in a fireproof safe for three months then moved offsite to a storage facility.

7. Tapes are kept offsite for one year.

8. Tape Catalogues are kept for one year.

9. Tapes will be labeled with the following:
   a. Barcode number
   b. Date
   c. Media Set
   d. Server
   e. Technician Name

10. In the event of inaccessibility to the local court unit either through building inaccessibility or a failure of access to the local network.
    a. A transactional copy of all critical file server data is replicated to multiple sites within the Wide Area Network.
    b. Those will provide access to the users to the latest data within a 24-hour period.
    c. Alternative servers are located at the satellite courthouse in Rockford, IL or should that site be inaccessible, remotely to the AO data center in San Diego.
    d. User movement and access to these systems will fail over automatically upon failure of the primary site and will be accessible to users either located at either physical site or by remote access through the Wide Area Network, should the users be granted that access.

6.5 Verification

1. Digital backups will be checked at least twice weekly to ensure the jobs are running properly.

2. Tape backup jobs will be checked at least twice a month.

3. All tapes removed for storage will be documented.

4. All tapes to be sent offsite will be inventoried and checked when returned to ensure all tapes are accounted for.

5. Test restores of backup media, both disk and tape, will be conducted at least once every month to ensure media can be restored properly when needed.

7. IT Security Training and Awareness

7.1 Introduction

IT Security Training is a necessary part of increasing the overall security of the United States District Court. With the ever-evolving security threat environment, it is necessary to educate all users when newly hired and annually to ensure the best practices and procedures are followed to protect the Judiciary's IT systems. All newly hired employees need to know the procedures and practices governing the usage of IT equipment managed by the court to start working safely and securely. All existing employees need to have their knowledge refreshed annually as IT security is an evolving field and new practices are developed. To best protect the Judiciary's systems, all users must have a basic understanding of the steps they can take to operate safely and securely using any IT equipment provided by the court and when accessing any government data regardless of location and device.

7.2 Scope

This policy will cover all newly hired, existing employees, and judges of the United States District Court for the Northern District of Illinois.

7.3 Policy

7.3.1 New Employee Orientation IT Security Training

1. All new employees must attend an IT Security Orientation provided by the Systems Department during their weeklong new hire orientations.

2. System access will not be granted until a new employee has completed IT Security Training satisfactorily.

3. The following must be discussed at all new employee IT Security training:
    a. Foundations of IT security
    b. Court IT policies and procedures applicable to new users
        i. Appropriate usage
        ii. Password Requirements

iii. Email Security
iv. IT Security incident notification

c. Authorized IT equipment usage
d. Responsibilities for assigned equipment
e. Basic defenses against the current security threat environment

4. The Systems Department is responsible for keeping a record that all new hires have been properly trained by appropriate staff.

5. The training curriculum will be reviewed and updated on an annual basis or as new and credible threats become apparent.

7.3.2 Annual IT Security Training

1. All employees must attend an annually organized IT Security Presentation if currently employed at the time of the scheduled training.

2. Any user that does not attend may have their access to IT systems revoked until they have satisfactorily completed the training and/or further disciplinary action from their superior.

3. The following topics must be discussed:
   a. Foundations of IT Security
   b. All applicable Court IT policies and procedures
      i. Appropriate usage
      ii. Password Requirements
      iii. Email Security
      iv. IT Security incident notification
   c. Authorized IT equipment usage
   d. Responsibilities for assigned equipment
      i. Desktop
      ii. Laptop
      iii. Other Mobile Devices
   e. Basic defenses against the current security threat environment
   f. IT data and equipment protection while traveling
   g. IT security in the courtroom
   h. Email, phone, and in-person IT security

4. The Internal Controls Analyst is responsible for keeping a record that all employees have been properly trained by appropriate staff.

5. The training curriculum will be reviewed and updated on an annual basis or as new and credible threats become apparent.

7.4 Procedure

7.4.1 New Employee IT Security Training

1. A properly trained representative of the Systems Department will conduct the training on the first day of new hire orientation.

2. The proper facility will be selected to ensure the presentation is easily seen by all attendees and that the speaker can be heard clearly.

3. The facility will be reserved for one hour to allow for the full presentation and answering additional questions from the trainees.

4. The facility must be secured from the public to prevent any sensitive IT security policies and procedures from being seen or overheard.
5. The Human Resources Department will ensure that all new hires are scheduled to attend the training during their new hire orientation week.

6. First-time login credentials will be provided at the end of the security training.

7.4.2 Annual IT Security Training

1. A properly trained representative of the Systems Department will conduct the training on a scheduled date that is at most one year from the previous training cycle.

2. The proper facility will be selected to ensure the presentation is seen by all attendees and that the speaker can be heard clearly.

3. The facility will be reserved for one and a half hours to ensure the full presentation is shown and allow room for questions.

4. The facility must be secured from the public to prevent any sensitive IT security policies and procedures from being seen or overheard.

5. It is the responsibility of the employee to register and attend one of the scheduled training sessions. Attendance is mandatory and will be tracked for auditing purposes.

6. The Systems Department representative will place a sign in sheet for employees to confirm their attendance in an easily visible place as well as remind users of their need to sign in and ensure that the sign in sheet is given to the designated record keeper.

7.5 Verification

7.5.1 New Hire Orientation IT Security Training

1. The Systems Department will keep a record of who attended training as part of their record of new hire setup.

2. The Systems trainer will be responsible for making the appropriate record update of the new hire list.

3. Any new hire that who did not sit successfully complete the security training will need to reschedule with the Systems Department before accessing any IT equipment.

4. The Systems trainer will provide a copy of the training record to the Internal Control Analyst who will maintain the records and audit them annually.

7.5.2 Annual IT Security Training

1. The Systems Department representative will require a sign in when entering the facility for the training.
2. The Systems trainer will provide a copy of the training record to the Internal Controls Analyst who will audit them.

3. Any employee who did not sign the log, but still attended the training will not be counted as having attended and the Clerk of Court is notified.

8. Network Management

8.1 Introduction

The network is the single most important connection at the Court. The network allows staff and judges to access files, research information on the internet, and send emails or messages. Therefore, it is necessary to ensure the network is managed efficiently to make certain the Court operates under normal conditions, secure transmissions, and minimize disruptions. This section of the policy details some of the requirements needed to ensure proper network management.

8.2 Scope

This Network Management policy applies to each of the organization's workforce members who have contact or potentially may have contact with the organization's data, applications, and computing resources. This includes, but is not limited to employees, contractors, vendors, service providers, volunteers, or any others who have or may come into contact with the organization's data, whether in a paid or unpaid capacity. Exceptions to this policy must be properly approved and documented in accordance with the organization's control exception policy.

8.3 Policy

The network is the single most important connection at the Court. The network allows staff and judges to access files, research information on the internet, and send emails or messages. Therefore, it is necessary to ensure the network is managed efficiently to make certain the Court operates under normal conditions, secure transmissions, and minimize disruptions.

The network boundary is defined as the connection from ILND's network to the Seventh Circuit network. This boundary will be defended by a firewall. The boundary firewall will be configured to allow the required traffic into and out of the ILND network. All traffic required by the AO to be blocked shall be blocked at the boundary. Any additional traffic may be blocked at the discretion of the Chief Judge, Clerk of Court, Systems Manager, or ITSO.

In order to ensure proper network management, IT Administrators must maintain an accurate account of all assets connected to the enterprise network. Administrators must actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. Network monitoring systems will be implemented and configured to alert staff when abnormal operations occur.

Documentation of the network layout will be maintained by the network staff which will include at least the following:

a. VLAN information
b. Subnetworks
c. IP Address Pool Assignments
d. Diagram of the network

The network documentation will be kept in a secure network share to prevent unauthorized viewing.

8.4 Procedure

1. The firewall configuration will be reviewed quarterly and a report will be provided to the Clerk of Court to ensure that all traffic is being filtered as required.

2. All blocked traffic documentation will be reviewed quarterly to determine if it is still applicable.

3. All network security measures shall be tested quarterly to ensure normal operations.

4. Network staff will monitor appropriate vendor communication lists and/or sites for update notices.

5. Once available, updates will be tested to determine viability and then applied to appropriate equipment within 90 days to ensure up to date security and operations.

6. The Court Unit will maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

7. Active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

8. The Court Unit will utilize the AO-provided inventory management tool, and use it to build a preliminary inventory of systems connected to the Unit's public and private network(s).

9. When the Court Unit is dynamically assigning addresses using DHCP, then the Court Unit will deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.

10. The Court Unit will ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.

11. The Court Unit will use client certificates to validate and authenticate systems prior to connecting to the private network.

12. The Court Unit will utilize the AO-provided inventory management tool and will devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
13. The Court Unit's software inventory tools will cover each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

8.5 Verification

1. Quarterly reviews will be documented for auditing purposes.

2. Blocked traffic will be tested by attempting to send the traffic and determining if it was blocked.

3. The network engineers will monitor update notice sources to ensure timely notice and updates.

4. Updated software will be marked as having been applied in the system's documentation.

9. Password Security

9.1 Introduction

Passwords are an integral part of daily IT usage. They secure user access to court systems and provide authorization to access files, functions, and other services. Passwords are not perfect and must therefore be protected by each person that possesses them to ensure that no intrusions and security incidents occur.

9.2 Scope

The following requirements and policies apply to all users in the United States District Court for the Northern District of Illinois.

9.3 Policy

1. It is recommended that passwords not be shared with any other person except when requested by Systems Department staff in the event of needed service.
    a. It is preferred that the password is given in person unless that cannot reasonably be accommodated.
    b. After the password is shared to Systems, it is recommended that the user change their password to ensure the required security. Systems staff will provide directions on how to change their password to the user once it is shared to a member of the Systems Department.

2. No user is allowed to login as any other user.

3. All users are required to report any potential loss of passwords to the help desk as soon as possible.

4. Accounts will lock for 30 minutes after five unsuccessful login attempts. Systems Department Staff may be contacted to have your account unlocked.

5. Screens will lock after 15 minutes of inactivity and will require a password to unlock the screen.

6. Password vaults recommended by the Administrative Office may be used for managing multiple passwords.

7. Passwords should not be written down unless the written password can be locked in a safe location.

8. Passwords may not be stored in plain text on any computer system or server.

9. Passwords should not contain personally identifiable information.

10. A single unique password should never be used for more than one account.
11. Personal passwords must never be mixed with Judiciary passwords.

12. Users may not use any default passwords or combination of the passwords that are issued by the Systems Department. They must change them immediately.

9.3.1 Requirements

1. Passwords shall be comprised of the following:
    a. Minimum of 8 characters in length
    b. Must contain at least one character from three of the following categories:
        i. Uppercase characters, i.e. A-Z
        ii. Lowercase characters, i.e. a-z
        iii. Numbers 0-9
        iv. Special characters: !@#$%&"'()*+,-./:;<=>?[\]^

2. Passwords cannot contain user names or user IDs

3. The five most recently used passwords cannot be reused

4. Passwords expire at 180 days and must be changed

9.4 Procedure

1. To ensure password standards are maintained, the Systems Manager and ITSO will ensure that an access control system is in place that mandates these requirements for all passwords in the court.

2. An auditing system will be maintained that monitors for password expiration and notifies of expiring passwords.

9.5 Verification

1. Quarterly, the ITSO will conduct a review of the password management systems in place to ensure they are configured according to this policy.

2. Password complexity and expiration requirements will be reviewed annually to ensure they are following adequate best practices from the AO.

10. Remote Access

10.1 Introduction

At times, some judges and employees will need to access the court network or DCN when not at the courthouse. This is done by using special software that allows the user to connect to the Virtual Private Network or VPN. This VPN access carries the risk of granting a user access from the outside of the standard access and security protocols. Therefore, it is necessary to ensure this access is restricted, audited, and secured.

10.2 Scope

This policy applies to all Clerk's Office employees including official court reporters when requesting, creating, and using a VPN or Virtual Private Network account. Judges automatically receive a VPN account.

10.3 Policy

10.3.1 Requesting a VPN Account

All users who need a VPN account must request one using the VPN Account Request Form provided by the Systems Department. In order for a VPN account to be approved, their manager must approve it and forward the approval to the Systems Manager.

10.3.2 Using a VPN Account

When using a VPN Account, the following must be ensured:

1. The computer used must have anti-virus security software installed and be fully updated
    a. Exceptions are handheld tablets and mobile phones

2. The device used must be fully updated for security

3. No other person may use the VPN account except the assigned user

4. The VPN account may only be used for official business

5. When conducting official business on a public internet source, a VPN must be used if possible

10.4 Procedure

1. A user will initiate the VPN request by filling out the appropriate form communicated either through an internal website or through systems staff.

2. Once filled out, the user will inform their supervisor that they have requested a VPN.

3. The Systems Manager and ITSO will review the application.

4. If approved, the VPN account shall be created.

5. The user will be notified the VPN account has been created and systems staff will instruct them on its proper usage and security.

10.5 Verification

1. Users with VPN access will be reviewed annually by the ITSO. Any user that has separated service or no longer requires the VPN will have access removed upon separation from the Court.

2. Any user found to be in non-compliance with this policy will be immediately barred from VPN access pending an investigation into the non-compliance and a review completed by the Clerk of Court and Chief Judge.

11. Security Log Management

11.1 Introduction

The purpose of this Log Management Policy is to ensure that ILND’s computer log data is securely and effectively generated, stored, analyzed, protected, and disposed.

11.2 Scope

This policy applies to all information technology assets within ILND’s local area network system boundary.

11.3 Policy

1. Log data from all IT systems will be generated, stored, analyzed, protected, and disposed of in accordance with documented processes, consistent with this policy.

2. Network Engineers, Systems Administrator, and Database Administrators will perform log management roles and responsibilities. Separation of duties will be observed to avoid potential conflicts of interest.

11.4 Procedures

1. Logging will be enabled where hardware or software supports feasible logging functionality, such as:
   a. network infrastructure devices (e.g., Intrusion Prevention Devices, switches)
   b. storage infrastructure (e.g., backup systems, data storage servers)
   c. applications (e.g., CM/ECF, Symantec Endpoint Protection)
   d. operating systems (e.g., Windows Server, Enterprise Linux)

2. ILND’s log management staff will:
   a. Develop a consistent and efficient process for analyzing log data.
   b. Review logs weekly during “normal” operations.
   c. Review logs promptly in response to an adverse event, e.g., upon receipt of an alert indicating a possible malware infection.
   d. Setup real-time alerting when practical to ensure potential threats are addressed in a timely manner.
   e. Develop a baseline of typical log entries to ensure malicious events can be recognized more easily and responded to quickly.

3. Events believed to be malicious or threatening must be reported to the Clerk of Court immediately.

4. Judiciary organizations should protect logs against unauthorized access, modification, and deletion. This preserves data integrity and ensures a record of system activities is available when needed by authorized administrators. Logging services should be included as part of the local continuity of operations plan (COOP) in the event of an incident.

5. To protect the logs, ILND staff will secure the processes that generate the log entries.

6. Ensure log source processing, executable files, configuration files, and other processes impactful to the generation of log data are protected from unauthorized access. For example, the maintenance of log files (updates to log processes, executable files, and configuration files) should be segmented on the LAN where only a limited number of individuals have access via unique logon IDs (different from their regular LAN accounts) with no rights to edit or delete log data.

7. Ensure only authorized individuals are allowed access.

8. Implement secure mechanisms for transferring log data.

9. Ensure log data is encrypted when transmitted off-site.

10. Provide adequate physical protection for logging mechanisms and stored logs.

11. Ensure network infrastructure devices and storage infrastructures are housed in a secure facility (e.g., data center or room where access is obtained via a secure key, cipher lock, security card, etc.) where only authorized individuals are allowed access.

12. Where feasible, ILND Log Staff should have at least 90 days of logs available online for analysis and have between one (1) and five (5) years available off-line (typically on an archive disk or backup tape).

13. Alerts will be issued when logs are close to reaching their retention capacity (e.g., 85% full) and when that capacity has been reached.

14. Retention schedules will be suspended when security logs are needed for an extended period in support of an investigation.

15. Where storage space allows, logs of production data actively used for real-time analysis, on-going review and periodic audits and assessments will be stored on-line for at least 90 days.

16. A backup of production logs will be made in the event that the logs may be compromised or damaged. Disk backups should be accessible for 6 weeks, and backed up to tape for off-site archival storage at least monthly.

17. Current tape backups will be kept off-site for Continuity of Operations recovery for at least six months. Archived tapes may be destroyed or disposed of after a one-year retention period.

18. ILND Log management staff will ensure that log data is disposed of after retention schedules have been met or when archive data is no longer needed for investigative purposes. ILND Log Management staff will suspend disposal activities in the event that logs are required in support of an investigation.

11.5 Verification

1. Annual Review of Procedure
    a. ILND’s log management staff will ensure processes are in place to generate, store, analyze, protect, and dispose of log data in a consistent manner.
    b. The procedures will be re-evaluated at least annually to ensure obsolete systems are removed and new systems are included.

12. Security Patch Management

12.1 Introduction

Patch management is an integral part of IT security operations. When firmware and software updates are released by the vendor, they generally include security patches to prevent their product from being compromised. These patches need to be applied in a consistent and frequent manner to ensure that security holes are being patched. This section outlines the policy and procedures to ensure proper patching of court IT systems.

12.2 Scope

This Security Patch Management policy applies to each of the organization's workforce members who have contact or potentially may have contact with the organization's data, applications, and computing resources. This includes, but is not limited to employees, contractors, vendors, service providers, volunteers, or any others who have or may come into contact with the organization's data, whether in a paid or unpaid capacity. Exceptions to this policy must be properly approved and documented in accordance with the organization's control exception policy.

12.3 Policy

1. The ITSO will subscribe to vendor notification lists and other sources such as US-CERT for alerts regarding patch availability.

2. The ITSO will schedule necessary updates for installation to the affected systems using the appropriate patch management tool.

3. The staff responsible for network operations will ensure that any patches or updates available for networking equipment will be installed no later than 180 days from the date of release bar any operating concerns.

4. All firmware and software in use by the court must be monitored for updates and patches.

5. All patches shall be tested on test machines before they are deployed to production systems to minimize the possibility of disruptions.

6. Court IT Administrators must continuously assess and remediate vulnerabilities. This includes continuously acquiring, assessing, and taking action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

11.4 Procedure

1. Patching will be conducted once a month or as mission critical security patches are released that the ITSO deems necessary to install. If an automated system is available for patching, this system will control as much of the process to minimize the need for IT staff to present. For non-automated patches, the patching will be conducted once a month during selected down time for

the system if necessary. Patches should be applied to all systems, even systems that are properly air gapped.

2. The Court Unit will run automated vulnerability scanning tools utilizing the AO-provided tool, against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to the responsible system administrator. Scans should look for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

3. The Court Unit will correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

4. The Court Unit will perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. The Court Unit will use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.

5. The Court Unit will subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization’s vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.

6. The Court Unit will monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.

7. The Court Unit will compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.

8. The Court Unit will establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.

12.5 Verification

1. IT staff will ensure patching has been completed by checking the patch management system logs for completion records.

2. IT staff will also select several systems to inspect to ensure the required patches have been applied.

13. Security Policy Exceptions

13.1 Introduction

No policy can cover every possibility and neither can it fully restrict them. Exceptions will periodically need to be granted for exceptional cases that require the waiving of a specific section of the policy. This section will detail the policy and procedures for properly requesting and, if found valid, maintaining the record of the exception.

13.2 Scope

This policy applies to all users in the USDC ILND and IT systems.

13.3 Policy

1. For exceptions to be granted, a requestor needs to initiate the request.

2. The final approval resides with the Chief Judge or Clerk of Court.

3. At no time is an exception to be granted that violates the *Guide to the Judiciary Policy* without the written approval of the Chief Judge.

4. All approved exception requests must be documented and kept with the Systems Department.

5. Exceptions may be revoked at any time by the Chief Judge.

6. Exceptions may only be requested by judges, Clerk of Court, or other management staff. Staff members may not request exceptions directly of the Systems Department, but may request their manager or judge (chambers staff) to request on their behalf.

7. Once an exception has been granted, it shall not be amended. An additional exception request will need to be generated.

8. If an exception is revoked, the revocation shall take place as soon as feasible, but no longer than the next business day.

9. All exceptions in effect will be kept in both digital and physical format for auditing purposes by the Internal Controls Analyst.

13.4 Procedure

1. To request an exception, the requestor must fill out the appropriate exception request form provided by the Systems Department.

2. The documented request must then be submitted to the ITSO or Systems Manager.

3. Once a request is received, the Systems Manager will forward to the Clerk of Court and Chief Judge.

4. The request will be reviewed for validity and be judged by three criteria.
    a. Significance of Security Risk, if any
    b. Feasibility of Implementation
    c. Business Necessity

5. Additional information may be requested at this time of the original requestor.

6. If denied, the Systems Manager will communicate to the requestor that the request was denied and the reasons why.

7. If approved, the Systems Manager or ITSO will communicate the exception approval and will then place the documented exception in the proper storage location.

8. If at any time, the exception is to be revoked, the revocation will be immediately communicated to the original requestor with the reasons why and when the exception will be revoked.

13.5 Verification

1. Once a year, the Internal Controls Analyst will review the currently held exceptions.

2. If an exception is found to be unnecessary, out of date, or for any other valid reason to be void, that exception shall terminate upon notification of the original requester.

3. If the exception is found to be valid, the Internal Controls Analyst will note the review date on the exception and approve it for one more year or until deemed necessary to expire.

14. Witness Protection

14.1 Policy

All Witness Security information is protected by the separate Pre-Trial and Probation Offices of the Northern District of Illinois. The US District Court for the Northern District of Illinois is not responsible for the protection of this information beyond what is applicable by federal law.

15. WLAN Security

15.1 Introduction

The court operates a wireless network to allow staff to continue operating with mobile devices when in the courthouses. Wireless networks are broadcast technologies and thus have more security concerns than the standard wired network. This section details the policy and procedures necessary for the security and safe operation of court wireless networks.

15.2 Scope

This policy applies to equipment and users of the court's wireless local area network.

15.3 Policy

1. The WLAN shall use the national wireless system for authentication controls.

2. The broadcast feature must be disabled for any private WLAN.

3. Public WLANs, where possible, shall not broadcast outside the boundary of the courthouse.

4. Private WLAN access shall be restricted to approved users and court issued devices.

5. Wireless Access Points will use the required security standards of the AO.

6. Users of the wireless network are responsible for making sure the devices they connect are up to date with security patches and running a current security application.

7. Wireless Access Point firmware will be updated whenever a security related patch is released or at least monthly for all other patches.

8. The wireless network controller, if any, will be updated whenever a security related patch is released or at least monthly for all other patches.

9. Access points connected to the DCN, and not authorized by the ILND Systems Department or other court units, are not allowed in the district court areas of the courthouses.

10. The Systems Manager and ITSO reserve the right to disconnect all rogue access points found in the ILND sections of the courthouse regardless of user if the device is interfering with court operations.

15.4 Procedure

1. The staff member responsible for maintaining the wireless network will monitor vendor websites for security related updates and apply them within 90 days of release if, after testing, no operating concerns are found.

2. The wireless network broadcast space shall be monitored for rogue access points at least twice a year to prevent unauthorized equipment interfering with normal operations.

15.5 Verification

1. The staff member responsible for maintaining the wireless network shall document when patches were applied to ensure a record for auditing purposes.

2. The wireless network shall be tested quarterly to ensure the requirements of this policy and any set by the AO are being followed.

16. Physical IT Security

16.1 Introduction

Physical access to sensitive Court IT systems must be restricted to authorized court IT staff in order to ensure security incidents are avoided and normal court operations are not interrupted. IT equipment still requires a physical location for it to sit and operate. Therefore, it must be protected from tampering by anyone not associated with the court Systems Department. This section details the physical security controls in place to protect court IT assets.

16.2 Scope

This section covers all court IT equipment necessary for IT operations.

16.3 Policy

The ILND Systems Manager and ITSO ensures physical security measures are in place for the protection of the organization’s information systems. Procedures for the implementation of physical and environmental protection safeguards are documented as part of the organization’s defense in-depth strategy for its IT security program. The Systems Manager and ITSO assign roles and responsibilities to IT staff for the implementation of physical security tasks.

1. All mission critical systems such as servers, network equipment, and anything else deemed critical for normal court operations is to be secured behind the appropriate lock that prevents any member of the public or unauthorized personnel from tampering or accessing the system.

2. The Court’s Procurement Department is responsible for maintaining the locks and security systems in place to protect IT equipment deemed necessary to protect.

3. Any combinations or keys to IT areas shall not be shared outside the Systems or Procurement Departments.

4. Unassigned physical access devices such as keys shall be maintained by the assigned Clerk’s Office employee and secured appropriately to ensure minimization of loss or theft.

5. When staff change, either through a change in role or separation from service, all security systems they had access to shall be changed and updated as necessary to prevent their access if applicable.

6. Procurement staff are responsible for auditing access logs on keyless doors and changing permissions as appropriate.

7. Any vendor providing support or maintenance, including federal non-court personnel, must be monitored by a member of the Systems staff if they are accessing a secured room unless granted an exception by the Systems Manager or they are contracted by the Procurement Department to perform work.

16.4 Procedure

The Systems Department will designate equipment as needing to be protected and will request the Procurement Department to physically secure the equipment.

16.5 Verification

The Systems Department will ensure that the equipment has been properly secured by testing the physical security through common attempts to bypass it without damaging the security devices.

17. IT Security Maintenance

17.1 Introduction

To ensure the proper functioning and regular daily operations of IT systems, it is necessary to have regularly scheduled maintenance to ensure updates, patches, and other items are installed and performed to keep the systems up to date and functioning normally. This section details the basic standards that all systems need in order to ensure long life operations and uninterrupted daily operations during normal business hours.

17.2 Scope

This section applies to all IT systems in use by the court.

17.3 Policy

1. Security patching will be performed according to the Security Patch Management section of the policy.

2. Non-security patches will be installed after testing along with the security patches at the regularly scheduled times.

3. A network monitoring system will be utilized to monitor all network equipment for abnormal operations.

4. A network monitoring system will be utilized to monitor all servers to alert on service disruptions or other abnormal operations.

5. All maintenance activities that will require downtime of regularly used systems will be documented and communicated to the entire court.

6. All scheduled downtime will be scheduled at times that will avoid the most disruption of operations.

7. All necessary spare hardware parts and software will be stored and managed by the inventory administrators.

8. Any maintenance that is to be performed by an outside vendor or contractor must be monitored by a member of the systems department if they are in a secure area they normally would not have access. At no time are they to be left alone in a secure area.

9. Systems staff will keep a record of all non-government vendors and contractors that enter secure areas to perform maintenance. This record will include at least the following:
    a. Name
    b. Company
    c. Phone Number

d. Area of entry
e. Time of entry
f. System(s) touched
g. Staff member monitoring

10. All records of contractor or vendor access will be kept for at least one year from the date of the work.

17.4 Procedure

1. The ITSO is responsible for ensuring updates and patching schedules are created. Patch installation operations may be delegated to appropriately trained staff.

2. System administrators will monitor applicable notification lists for system upgrade alerts and then apply them as applicable.

3. The Systems Manager or ITSO, will assign members of the department to inspect and/or clean data closets and the data center as needed.

4. Any non-government vendor or contractor that needs to enter a secure area will be assigned to a member of the systems department who will monitor them while they are working.

5. The assigned member will also be responsible for completing the documentation and filing it with the ITSO.

17.5 Verification

1. The ITSO will review the patch schedules and installations to ensure they are completed according to the desired schedule.

2. The Systems manager and/or the ITSO will review all requests for maintenance for systems in secure areas and ensure the correct documentation has been created.

3. At least once a year, the ITSO will review the documented maintenance performed and dispose of old records as needed.

18. Media Sanitization and Information Disposal

18.1 Introduction

Media and other information can be compromised if not properly disposed of when removing data and equipment from the courthouses. This section will detail the policy and procedures that govern the proper erasure and disposal of all government information off any IT system or device that is going to be sold or removed from the courthouses permanently.

18.2 Scope

This section covers all media and equipment to be disposed of by the Court's Systems Department.

18.3 Policy

1. All storage media that requires destruction shall be collected by the Systems Department until such an amount is collected that the Procurement Department can then dispose of it through a vendor securely.

2. Certificates of destructions shall be requested for all media disposal operations conducted by an outside vendor.

3. Hard disk drives present in any system to be disposed of shall be wiped according to appropriate best practices for the drive before being placed in storage for reuse or provided with the disposed device. Any non-removable hard disk drive must be wiped before disposal of the item.

4. Any damaged or non-functional hard disk drive that cannot be feasibly wiped must be destroyed in accordance with best practices. The Procurement Department will be responsible for destruction of media and disks through an outside vendor.

5. All paper documents that contain IT information sensitive to internal operations must be either shredded by the Systems Department or deposited in one of the provided shred bins.

6. All information that is defined as a federal record must be preserved according to the Federal Records Schedule.

18.4 Procedure

1. The designated IT staff responsible for disposal shall collect and secure all media and information pertinent to be destroyed or sanitized.

2. Once a sufficient amount has been collected, the media destined for destruction shall be provided to the Procurement Department for proper disposal.

3. All media that can be erased, such as hard disk drives, must be wiped no fewer than three times to ensure data destruction.

4. All media that is to be destroyed shall be documented by the designated staff member.

18.5 Verification

1. Once media has been destroyed and a certificate of destruction has been provided, the IT staff member responsible for disposal shall confirm the certificate matches the documented record of media.

2. This certification shall be maintained for one year for auditing purposes.

3. Any equipment or software used to erase securely data shall be tested annually to ensure it is functioning normally.

Definitions

Access Point
An access point is a device that allows wireless devices, such as laptops, tablets, and cell phones, to connect to a network.

AO
The Administrative Office of the United States Courts

Backup
In information technology, a backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.

Cell phones
A cell phone is any portable telephone that uses cellular network technology to make and receive calls.

CERT
The Computer Emergency Response Team

CM/ECF
Case Management and Electronic Case Files System

Configuration
The arrangement or set-up of the hardware and software that make up a computer system.

COOP
Continuity of Operations Plan

Deployment
The processes involved in getting new software or hardware up and running properly in its environment.

Desktops
A desktop computer is a personal computer designed for regular use at a single location on or near a desk or table due to its size and power requirements.

DRP
Disaster Recovery Plan

Email
Messages distributed by electronic means from one computer user to one or more recipients via a network.

Encryption
The process of converting information or data into a code, especially to prevent unauthorized access.

Firmware
Firmware is used to run user programs on the device and can be thought of as the software that allows hardware to run.

Hardware
Computer hardware is the collection of physical parts of a computer system.

ILND
Illinois Northern District

IM
Instant Messaging

Instant messaging
Instant messaging is a way of chatting between two or more people by typing text. The text is then sent by computers over a network, such as the internet, in real time.

ISCPs
Information System Contingency Plans

IT
Information Technology

ITSO
Information Technology Security Officer

JASIRC
Judiciary Automated Incident Response Capability

Laptop
A computer that is portable and suitable for use while traveling.

Log
A record of computer activity used for statistical purposes as well as backup and recovery.

Mailbox
A computer file in which email messages received by a particular user are stored.

Media
Materials that hold data in any form or that allow data to pass through them, including paper, transparencies, multipart forms, hard, floppy and optical discs, magnetic tape, wire, cable and fiber.

Network
A number of interconnected computers, machines, or operations.

Security Training
A formal process for educating employees about computer security as it relates to the United States District Court and its policies.

Software
The programs and other operating information used by a computer.

SSID
The name assigned to a Wi-Fi (wireless) network. All devices in the network must use this case-sensitive name to communicate over Wi-Fi.

Storage
The retention of retrievable data on a computer or other electronic system.

Streaming
A method of transmitting or receiving data (especially video and audio material) over a computer network as a steady, continuous flow, allowing playback to proceed while subsequent data is being received.

Systems
The Information Technology (IT) department for the Court.

Technical support
A service provided by a hardware or software company that supplies registered users with help and advice for their technology products.

Technician
A person employed to look after technical equipment.

USDC
United States District Court

User
A person who uses or operates something, especially a computer or other machine.

Wireless Network Broadcast
In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network.

Wireless Network Controller
A device that administers all the access points connected on a network to centrally control, monitor, and manage them.

WLAN
A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method within a limited area such as a home, school, computer laboratory, or office building.