Administrative Office of the Courts

Judicial Information Systems

Information Security Policy

January 2024

Contents

PURPOSE

The purpose of this Policy is to describe the security guidelines that the Maryland Judiciary must consider when protecting the confidentiality, integrity and availability of Judiciary owned information.

The Judiciary supports and utilizes industry leading information security practices within the Policy, to include the Federal National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) Critical Security Controls Frameworks. The NIST Framework is a collection of nationally recognized security standards and covers cybersecurity functional areas that offers guidance on the identification, protection, detection, response and recovery mechanisms used to protect an organization's infrastructure and assets. CIS is an independent not-for-profit organization that develops and promotes best practices to help governments and businesses protect against cyber threats. The NIST and CIS Controls are designed to complement one another and provide the highest degree of information security standards and guidance available.

This Policy establishes the general requirements and responsibilities for protecting Judiciary systems and information.

SCOPE

This Policy applies to anyone provided access to Judiciary technology or information assets including but not limited to information that is generated, received, stored, transmitted or printed.

The policy scope encompasses:

- All courts, units and departments, and personnel of the Judicial Branch of the State of Maryland that access the Judicial Information Systems (JIS) network.
- All activities and operations required to ensure data security. This includes:
  - facility design,
  - physical security,
  - disaster preparedness and business continuity planning,
  - use of hardware and operating systems or application software,
  - destruction of data, media, or equipment, protection of copyrights, software licensing agreements, and other intellectual property rights.

AUTHORITY

The Chief Justice of the Supreme Court of Maryland is the establishing authority for this Policy with the advice and guidance of the Judicial Council.

The Chief Justice of the Supreme Court of Maryland has the authority to exempt a category of users from any requirement of this Policy.

All subsidiary information security policies, protocols, programs, and procedures implemented by JIS derive their authority from this Policy.

SECTION 1: Preface

Information and information technology (IT) systems are essential assets of the Maryland Judiciary and vital resources to Maryland citizens. These assets are critical to the services that the Judiciary provides to citizens and local and federal government entities. All information created with Judiciary resources for Judiciary operations is the property of the Maryland Judiciary. All users of the Judiciary's IT assets, including contractors and other third parties, are responsible for protecting those assets from unauthorized access, modification, disclosure, damage and destruction. This Policy sets forth a minimum level of security controls that, when implemented, will provide for the confidentiality, integrity, and availability of Judiciary IT assets.

In general, the Judiciary will adopt information security leading practice standards and guidelines. This Policy developed to secure the Judiciary's IT assets will, where appropriate, refer to a particular standard. Judiciary security procedures will be documented to ensure compliance with the Policy. The Policy will be reviewed on an annual basis.

SECTION 2: Roles and Responsibilities

This Policy sets the minimum level of responsibility for the following individuals and/or groups:

- Administrative Office of the Courts (AOC)
- Court Technology Committee of the Judicial Council (CTechCom)
- Chief Information Officer
- Information Security Officer
- Chief Technology Officer
- Users of Judiciary Assets

2.1 Administrative Office of the Courts (AOC) / CTechCom

- The Administrative Office of the Courts will serve as the governing body to oversee the Information Security Policy.
- CTechCom will be responsible for reviewing this Policy annually and for reporting findings and recommendations to the Judicial Council at least annually. The AOC and JIS will provide guidance and recommendations regarding IT security to CTechCom.

2.2 Chief Information Officer (CIO)

The Chief Information Officer shall:

- Ensure that security is considered and integrated into all Judiciary information technology plans and objectives.
- Serve as the Liaison for JIS on the CTechCom.
- Serve as the authorizing official and signs the Authorization to Operate (ATO) for new application systems at an acceptable level of risk into the organization.
- Establish and enforce IT governance policies, standards, and procedures.
- Ensure compliance with regulatory requirements and industry standards.
- Implement and maintain robust cybersecurity measures to protect the organization's data and information assets.
- Monitor project progress and manage risks.

2.3 Information Security Officer (ISO)

The JIS Information Security Officer shall:

- Ensure the JIS business continuity plans (BCP) and disaster preparedness (DP) plans for critical JIS systems are reviewed, updated and exercised (tested) annually.

- Review and update this Policy annually.
- Develop, implement, and continue to mature the Security Program.
- Present changes and updates to this Policy and the Security Program to the CTechCom by April 1st.
- Employ the appropriate measures to assure and demonstrate compliance with this Policy.
- Conduct regular external and internal vulnerability assessments to verify security controls are working properly and to identify risks.
- Assure the confidentiality, integrity, availability, and accountability of all Judiciary electronic information assets while it is being used, processed, stored, or transmitted, and the security of the resources associated with those processing functions.
- Assists in the orchestration of Internal and External audit requests of JIS operations
- Incorporates new security requirements as enacted through Maryland state statute and regulation.
- Develop, implement, and maintain an incident management process.
- Assume the lead role in resolving Judiciary security and privacy incidents.
- Provide support and guidance on information security issues to all Judiciary entities.

2.4 Chief Technology Officer (CTO)

The Chief Technology Officer shall:

- Evaluate, prepare, and deploy systems that support this policy and the Information Security Program of the Judiciary.
- Reviews all new technology initiatives, systems, applications and technologies for security and architectural efficacy.
- Evaluate and select vendors and service providers that will contribute to the information security posture of the Judiciary.
- Define and maintain the technical architecture ensuring scalability, reliability, and security.
- Implement security controls and technologies to protect the organization's networks, systems, and data.
- Provide support and technical expertise related to information security initiatives.

2.5 Users of Judiciary Assets

All users of the Judiciary’s IT assets are responsible to:

- Be aware of and comply with this Policy and associated or subsidiary standards, procedures and guidelines.
- Understand her/his responsibilities for protecting IT assets of the Judiciary. Use IT assets and resources only for authorized business purposes as defined by policies, laws and regulations of the Judiciary or the State.
- Be accountable for her/his actions relating to her/his use of all JIS managed IT systems and information.
- Be responsible for her/his assigned account. Users are prohibited from sharing her/his account credentials with others, including with other Judiciary personnel, except as otherwise provided by Policy.

SECTION 3: Asset Management

An inventory of all critical IT assets is required as directed by the Chief Information Officer. Accountability for assets helps to ensure that appropriate protection is maintained. Designated owners shall be identified (Data Owners and Custodians) for all critical assets and assigned responsibility for the maintenance of appropriate controls.

3.1 Inventory of Assets

Compiling an inventory of assets is an important aspect of risk management. JIS must identify Judiciary assets and the relative values and importance of these assets.

Based on this information, JIS can then provide appropriate levels of protection. Inventories of the critical assets associated with each information system should be documented and maintained. Asset inventories shall include, at a minimum, a unique system name, a designated owner and a description of the physical location of the asset. Examples of assets associated with information systems are:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, disaster preparedness plans, archived information.
- Software assets: application software, system software, development tools and utilities.
- Physical assets: network equipment including servers, routers, switches, network devices, communication devices, network printers, etc.
- Desktop computing equipment must adhere to the inventory controls as outlined in the AOC Inventory Control Manual.

3.2 Data Type Classification

This Policy pertains to all information within the Judiciary's IT systems that is processed, stored, transmitted or shared. Data Owners and Custodians must adhere to this Policy and educate users who may have access to confidential information for which they are responsible.

All Judiciary IT information is categorized into three main classifications with regards to criticality, severity and business value:

- Public
- Confidential
- Private

Public information is information that has been declared publicly available by law or Rule. Public records are any records that are made or received by a covered public agency in connection with the transaction of public business.
Confidential information is non-public information that is defined by law or rule that must be withheld from public access. This may include, but is not limited to, Personally Identifiable Information (PII), sealed information and Parties Only information. The unauthorized release of confidential data could result in a significant adverse impact on the Judiciary's mission, safety, finances, or reputation. Therefore, additional security precautions must be taken when storing. transmitting, and/or processing such data.

Private information is any sensitive, non-public information that should not be disclosed to the public as it would increase the risk to the confidentiality, integrity and availability of Judiciary information.

As defined by the State of Maryland, Personally Identifiable Information means, in digital or physical form:

A full name, or first initial and last name, in combination with:

- A Social Security number.
- A driver's license Number, a state identification number, passport number, military identification number, or any other individual identification issued by a State or Federal unit.
- A Financial or other account number, a credit card number, or debit card number that, in combination with any required security code, access code, or password would permit access to an individual's account
- Characteristics of classifications protected under federal or State law; or
- Biometric information including an individual's physiological or biological characteristics, including an individual's deoxyribonucleic acid, that can be used, singly or in combination with each other or with other identifying data, or to establish individual identity.
- If a user is uncertain of the classification of a particular piece of information, the user should contact their manager for clarification.

To the extent required by law or rule, all confidential information should be clearly identified as such and will be subject to marking and handling guidelines.

3.3 Guidelines for Marking and Handling Confidential Judiciary Information

To the extent required by law or rule, Judiciary confidential information shall be protected and marked in accordance with the data sensitivity. Users shall not electronically store data that cannot be adequately secured against unauthorized access.

3.4 Security Categorization Applied to Information Systems

JIS will classify systems consistent with the classification of the data within the system. When an IT System is shared between the Judiciary and external parties, the highest risk and sensitive level of data classification will determine the classification of the IT System.

SECTION 4: Security Controls Overview

All Judiciary IT assets (hosted on the Judiciary network or a 3rd party offsite premise) used for receiving, processing, storing and transmitting Judiciary data must be protected in accordance with these controls. Information systems include the equipment, facilities, and people that handle or process Judiciary data.

These security controls are categorized into three types:

- Managerial
- Operational
- Technical

Managerial security controls focus on managing organizational risk and information system security and devising sufficient countermeasures for mitigating risk to acceptable levels.
Managerial security controls include, but are not limited to, risk management and project management.

Operational security controls focus on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or a group of systems. Operational security controls require technical or specialized expertise and often rely on managerial and technical controls. Operational security controls include awareness and education, configuration management, service interface agreements, contingency planning, incident response, maintenance, media protection, physical and personnel security, system and information integrity, and system development life cycle methodology (SDLC).

Technical security controls focus on operations executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system. Technical security controls include access control, audit and accountability, authentication and authorization, user authentication and password requirements, and system and communications.

SECTION 5: Managerial Level Controls

5.1 Risk Management

- Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for the Judiciary to successfully implement and maintain an acceptable level of security. A risk management process must be implemented to assess the acceptable risk to Judiciary IT systems.
- As a part of a risk-based approach used to determine suitable security safeguards are in place for IT assets, the Judiciary shall utilize security frameworks, tools and techniques to perform assessments for security weaknesses, threats and vulnerabilities and recommend appropriate, cost-effective controls to achieve and maintain an acceptable level of risk.
- In addition, the Judiciary will utilize third party services to conduct a security risk assessment every two (2) years. The assessment shall be performed by an independent third party with cybersecurity expertise to determine whether the Information Technology services being provided by Judicial Information Systems meet relevant NIST cybersecurity standards on the acceptable risk to Judiciary IT assets.
- In the event an identified risk cannot be fully remediated, mitigation steps must be taken to reduce the risk. The risk and steps taken to mitigate the risk must be formally documented, accepted, and approved, by the CIO. All Risk Acceptances will be reviewed annually or until the identified risk no longer exists.

5.2 Project Planning

- Judiciary Information Technology projects, including system development, enhancement, maintenance, and infrastructure activities shall be managed to ensure that delivered solutions are consistent with this Policy.
- Plans for executing IT projects should include a general process for addressing IT security controls. JIS shall ensure that all major IT development or infrastructure projects have a corresponding project plan that addresses the security control requirements within this Policy. JIS Information Security shall be an integral part of this planning process.

SECTION 6: Operational Level Controls

6.1 Security Education and Awareness

- JIS is responsible for educating users on security threats that may impact secure operations of the JIS network and provide information on mechanisms to protect against these threats. The Judiciary must ensure all active JIS network Windows users regularly participate in a formal security education and awareness training program, to include phishing campaigns. The program must have the ability to track completion of required security training assignments and report on non-compliance. The formal program must also include learning opportunities for users to independently explore information on safe computing practices.
- The training program shall include targeted training, at least once a year, that is directed towards Privileged account holders, Developers, and Executives

.

6.2 Configuration Management

System hardening procedures shall be created and maintained to ensure up-to-date security leading practices are deployed for all IT operating systems, applications, databases, network, and hardware devices. All default system administrator passwords must be changed. JIS shall implement an appropriate change management process to ensure changes to systems are controlled by:

- Developing, documenting, and maintaining current baseline configurations.
- Network devices, host and guest operating systems, and databases must be patched and updated for all security related updates/patches using automated tools when possible.
- Baseline images for servers and workstations must be established and reviewed annually.
- Developing, documenting, and maintaining current inventories of the components of information systems and relevant ownership information.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.
- Analyzing potential security impacts of changes prior to implementation.
- Authorizing, documenting, and controlling system level changes.
- Restricting access to system configuration settings and provide the least functionality necessary.
- Prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting confidential information.
- Maintaining backup copies of hardened system configurations.

6.3 Network Connection Management

Except for ‘NetworkMaryland’ provided connections, external network connections shall be permitted

only after all approvals are obtained consistent with this Policy and shall be managed as agreed to by the Judiciary and the untrusted entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system that includes:

- Purpose and duration of the connection as stated in the agreement, lease, or contract.
- Points-of-contact and cognizant officials for both the Judiciary and untrusted entities.
- Roles and responsibilities of points-of-contact and cognizant officials for both Judiciary and untrusted entities.
- Security measures to be implemented by the untrusted organization to protect the Judiciary's IT assets against unauthorized use or exploitation of the external network connection.
- Controls to detect and monitor for the connection of unauthorized devices to a JIS system.
- Requirements for notifying the JIS Information Security Officer within two business days of a security incident on the network.

Network Maryland-provided Internet and SwGI Connections

All Maryland Judiciary connections utilizing the Maryland Department of Information Technology (DoIT) 'NetworkMaryland' network for Internet or data transport services or are using the Statewide Government Intranet (SwGI) to host or share data across the network must include the following security controls:

- Maintain a network boundary capable of performing packet filtering to ensure that only authorized traffic is permitted.
- Enable intrusion detection and prevention systems on each interface.
- Monitor the firewall logs for each connection.
- Prohibit direct external access to high-risk or frequently abused network protocols.
- High-risk and commonly abused ports must not be used.

6.4 Disaster Preparedness Plan

JIS must maintain and test an IT Disaster Preparedness plan for all JIS systems determined to be essential for ongoing business. Maintenance and annual testing of the plan will minimize the impact of interruptions of information technology service delivery caused by events ranging from a single disruption of business to a disaster. Disaster Preparedness Plan maintenance should be incorporated into the JIS architecture review and change management processes to ensure plans are kept current.

Primary Components of an IT Disaster Preparedness Plan are:

- Identification of a disaster preparedness team
- Definitions of preparedness team member responsibilities
- Documentation of each critical system including:
    - Purpose
    - Hardware
    - Operating System
    - Business and Middleware Application(s)
    - Data
    - Supporting network infrastructure and communications
- System restoration priority and dependency list
- Identification of alternate site including contact information
- Description of current system back-up procedures
- Description of back-up storage location
- Description of back-up testing procedures (including frequency)
- System Recovery Time Capabilities RTC (time between unexpected failure to normal operations)

- System Recovery Point Capabilities RPC (how current the data should be at recovery)
- Procedures for information technology service delivery at alternate and primary production JIS site

6.5 Incident Management

Incident Management refers to the processes and procedures JIS implements for identifying, responding to, documenting and managing information security incidents. A security incident within the JIS managed networks is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices.

6.6 Maintenance

- JIS must identify, approve, control, and routinely monitor the use of information system maintenance tools and remotely executed maintenance and diagnostic activities. Only authorized personnel are to perform maintenance on information systems.
- JIS must ensure that system maintenance is scheduled, performed, and documented in accordance with manufacturer or vendor specifications and this Policy.

6.7 Media Protection

- The purpose of this section is to ensure proper precautions are in place to protect confidential information stored on media.
- Removable media containing sensitive or confidential information must be encrypted at the device or file level.
- JIS shall restrict access to system media containing confidential information to authorized individuals. Media containing confidential information shall be physically controlled and securely stored. JIS must protect and control confidential system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
- Throughout the lifecycle of IT equipment, there are times when JIS will be required to relinquish custody of the asset. The transfer of custody may be temporary, such as when equipment is serviced or loaned, or the transfer may be permanent; examples being a donation, trade-in, lease termination or disposal.
- To eliminate the possibility of inadvertently releasing residual Judiciary confidential information, the Judiciary will have a formal procedure for media sanitization.

6.8 Physical and Personnel Security

Physical access to information technology processing equipment, media storage areas, and mass media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized access to these areas.

The Judiciary must:

- Secure IT areas with controls commensurate to the risks
- Ensure secure storage of media
- Obtain personnel security clearances where appropriate

Physical access controls must be in place for the following:

- Data Centers
- Areas containing production servers
- Networking cabinets and wiring closets
- Power and emergency backup equipment

Access to data centers and secured areas should be limited to those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas.

Authorization should be:

- Based on frequency of need for access.
- Approved by the Administrative Official responsible for the secured area.

The Administrative Official or designee for each data center or secured area is responsible for:

- Ensuring that all removable media are physically secured.
- Ensuring proper employee/contractor identification processes to include periodic recertification are in place.
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems.
- Ensuring that any physical access controls are auditable.

6.9 System and Information Integrity

- JIS shall implement system and information integrity security controls including vulnerability remediation, information system logging and monitoring, information input restrictions and information output handling and retention.
- JIS must protect against malicious code, virus or malware by implementing procedures and solutions that, to the extent possible, includes a capability for automatic updates. Intrusion detection/prevention tools and techniques must be employed to log, monitor and review system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.
- JIS systems must restrict information input to authorized personnel (or processes acting on behalf of such personnel) responsible for receiving, processing, storing, or transmitting confidential information.
- JIS shall utilize mechanisms to validate the integrity of the data sent to partners in justice and receive acknowledgement of successful transmission and delivery. Files containing confidential information may be removed from the system once the receiving party acknowledges receipt of the transmitted information. Acknowledgements for transmission and delivery must be stored for internal/external inspection as outlined in section 7.2, Audit & Accountability Controls.
- Information system security alerts/advisories for critical software must be regularly reviewed and applied as appropriate by the person(s) assigned responsibility for software administration.
- External and internal vulnerability assessments must be performed to verify security controls are working properly and to identify risks. Identified vulnerabilities must be categorized in accordance with severity level. Vulnerabilities with a severity level of critical or high must be acknowledged in a timely manner. Vulnerabilities that cannot be remediated in a timely manner must undergo a plan of action and milestones to monitor residual risk.

6.10 System Development Life Cycle Methodology

All Judiciary systems must include IT security as part of the JIS system development life cycle (SDLC) management process. The JIS SDLC policy applies to all JIS approved projects. This process should include, where applicable:

- Create a system security plan (SSP) that includes system criticality.
- Conduct a risk assessment and baseline of security controls.
- Create detailed design document (DDD) – examples include.
    - System architecture
    - Database design
    - Description of all the platforms, systems, services, and processes the product would depend on
    - Description of relationships between the modules and system features
    - Converts user requirements and stories into high level solution.
    - Used to create an understanding of process and data flow within the system.
    - Overall high-level application and network architectural design between the various modules in the system.
- Create technical design documents (TDD)
    - Provides information for building the product and the core configuration.
    - Component-level design process.
    - Provides the details and definitions for the actual logic for every system component.
- Implement requirements for ensuring authenticity and protecting message integrity in applications.
- Implement processes to control the installation of software on operating systems.
- Implement procedures to select, protect and control test data. Do not use test data in a production environment or use production data in a test environment without careful consideration.
- Limit access to program source code and place source code in a secure environment.
- Implement change/configuration control procedures to minimize the corruption of information.
- Develop a system user access certification and recertification plan on a regular schedule.
- Submit a formal letter requesting an authorization to operate (ATO) for a new system to the CIO or designee and Information Security Officer for approval.

6.11 Backup Plans

- Shall include backup and recovery processes.
- Shall include continuous backups with a predefined frequency based upon the recovery goals to include daily weekly or custom scheduling.
- A defined retention policy should be established for data archive.
- Backups must include immutable copies.
- At a minimum backup shall be replicated to an offsite secured data center.
- Backup copies must include protection with encryption at rest and inflight.
- Backup restoration tests shall be completed regularly to check the confidentiality, integrity, and availability of the data.
- Backups shall include logging capabilities to monitor activity.
- Least privileged shall be used in the protection and access.
- When able, multi-factor authentication shall be implemented when logging into the backup platform.

SECTION 7: Technical Level Controls

7.1 Access Control Requirements

- The Judiciary must manage user accounts, including activation, deactivation, changes and audits.
- The Judiciary must ensure that only authorized users (employees or agency contractors) have access to confidential information and that such access is strictly controlled, audited, and that it supports the concepts of “least possible privilege” and “need to know”.
- The Judiciary must ensure that systems or business processes, where feasible, enforce separation of duties through assigned access authorizations.
- Information systems must display the approved use agreement before granting system access.
- JIS must ensure that unauthorized users are denied access by ensuring that user sessions time out or initiate a re-authentication process after an approved period of inactivity.
- JIS must authorize, document, and monitor all remote access capabilities used on its systems. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption for transmission of data and authentication information.
- JIS must develop formal procedures for authorized individuals to access its information systems using a remote connection.
- JIS must authorize, document, and monitor all wireless access to its information systems. Wireless security guidelines are documented in Section 15.

7.2 Audit & Accountability Control Requirements

- The following minimum set of events/actions on systems that are categorized as critical or confidential, shall be logged and kept, to support the audit or investigation of activities, as required by all applicable State and Federal laws or regulations. System owners must ensure that audit information is archived for 3 years unless otherwise specified in the AOC records retention and disposal schedule.

    - Additions, changes, or deletions to data produced by the system.
    - Authentication and Authorization processes.

- A process must be established to detect and where feasible, alert the responsible parties in the event of an audit processing failure and appropriate remediation steps must be taken.
- Information systems must be configured to allocate sufficient audit record storage capacity to record all required auditable items.
- Procedures must be developed to routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to responsible parties for prompt resolution.
- System owners must protect audit information and audit tools under their control from unauthorized access, modification, and deletion.

7.3 Authentication & Authorization Control Requirements

- Users, devices, and processes must use standard authentication via the assignment of unique user accounts using standard authentication methods such as passwords, tokens, etc.
- Use of Multi-factor authentication is required for all users who use remote access technology to connect to the Judiciary’s network.
- Each user is responsible for all activities performed using his/her account credentials.
- Each user is responsible for their assigned account. Users are prohibited from sharing their account credentials with others, including other Judiciary personnel except as otherwise provided by policy (see Exhibit 1).
- Users must validate their identity when requesting a password reset or account unlock. The validation process must be at least as strong as when originally established.
- Shared functional accounts are prohibited unless formal approval is obtained from JIS Information Security.
- All requests for accounts must follow the formal documented procedures.

- The Judiciary must manage user accounts assigned within its information systems. Effective user account management practice includes:
- Obtaining authorization from appropriate officials to request user account creation, modification and deletion.
- Performing periodic recertification of application users and their associated privileges based on level of sensitivity.
- Timely disablement of user accounts when no longer required.
- Information Systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

7.4 User Authentication & Password Requirements

Passwords must meet the following construction, usage and change requirements:

- The password must not be the same as the user id.
- Passwords must not be stored in clear text
- System design must prohibit or obfuscate password display during entry of clear text passwords
- Temporary passwords must be changed at the first logon
- Passwords must be complex to the extent possible supported by the system (e.g., contain a combination of at least three of the following four elements: upper case letter, lower case letter, number, or special character)
- User-level passwords must be changed at required intervals
- Password reuse must be prohibited by not allowing reuse of the last ‘n’ passwords, where ‘n’ is a number (e.g., 10) defined in the system password configuration
- User ids associated with a password must be locked after a specified number of failed login attempts
- User ids associated with a password must be automatically disabled or locked after a specified period of account inactivity
- User’s identity must be validated when a user password reset is requested
- Where possible, Multi-Factor Authentication (MFA) must be implemented on public-facing systems.

Functional/System accounts may have unique authentication and password requirements that cannot comply with these requirements. Mitigating security controls must be in place that reduce risk to an acceptable level. These controls must be formally approved and documented.

7.5 System & Communication Control

- Information systems shall separate front end interfaces from back-end processing and data storage, where feasible.
- Information systems shall prevent unauthorized and unintended information transfer via shared system resources by adhering to the concept of least privilege and ensuring functional accounts are not shared across applications.
- Information systems shall be configured to monitor and control communications at the external boundaries of the information systems and at key internal boundaries within the systems.
- Information systems must protect and secure all confidential information during electronic transmission.
- Acknowledgement files of transmitted confidential data must be retained.
- When Public Key Infrastructure (PKI) is used, JIS shall establish and manage cryptographic keys using secure mechanisms with supporting procedures.
- Whenever there is a network connection external to the system, the information system shall terminate the network connection at the end of a session or after an approved period of inactivity.

SECTION 8: Virtualization Technologies

- JIS must install, configure, and deploy virtualization solutions to ensure that the virtual environment is as secure as a non-virtualized environment and in compliance with all relevant JIS Policy and Procedures.
- Access to the virtualization management system should be restricted to authorized administrators only.
- Install all virtualization software updates as they are released by the vendor on a regularly scheduled basis. Centralized patch management solutions can also be used to administer updates.
- Restrict administrative access to all virtualization management interfaces.
- Protect all management communication channels using segmentation or other methods of isolation to segregate the management network.
- Synchronize the virtualized infrastructure to a trusted authoritative time server.
- Install all guest Operating Systems updates on a regularly scheduled basis.
- Virtual machines must include descriptions for what is hosted or installed on the guest operating system.

SECTION 9: Cloud Computing Technologies

Cloud computing is a model for enabling computing resources (e.g., networks, servers, storage, applications, and services). Judiciary implementation of a cloud-based solution must be implemented to ensure the solution is as secure as on premise and follows relevant JIS Security Policy and Procedures. All Cloud Computing platforms to include but not limited to Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Dedicated Hardware services require a security and architectural review prior to implementation.

All cloud service provider contracts should establish terms and conditions for services which may include, but is not limited to:

- Service Level Agreements (SLA) and penalties for non-compliance
- Non-Disclosure Agreement
- Right to Audit Clause
- Data ownership
- Third Party attestation reports (example Service Organization Control (SOC 2 Type II)
- Attestation reports for systems holding confidential data must be requested on an annual basis and submitted to Information Security for review.
- Data in transit to and from the cloud, as well as data stored in the cloud must be encrypted.
- When possible, third-party software must comport with the user authentication and password requirements as outlined in Section 7.4 of this Policy.
- Privileged access accounts accessing for the management or use in the cloud, must use multi-factor authentication when available.
- Cloud computing technologies must not be engaged without consideration for an exit strategy in the event the Judiciary must disengage from the vendor or service.
- The hosted service must be incorporated into the business continuity and disaster recovery plans.

SECTION 10: Information Systems Contracts

- Contracts shall be written to ensure vendors and Service Providers agree to adhere to JIS Security Policy and Procedures and all applicable Rules, State and Federal laws or regulations.
- All hardware and software purchases shall be procured through qualified sources in accordance with AOC procurement policies and guidelines, unless otherwise authorized by the CIO or designee in this area.

SECTION 11: Mobile Devices

Any user receiving Judiciary data or connecting a mobile device to the Judiciary network must comply with the JIS Security Policy and Procedures and all applicable Rules, State and Federal laws, regulations, and mandates.

- All Judiciary issued mobile devices must be managed by the mobile device management platform.
- All Judiciary issued devices must be kept current with the latest operating system and install the most recent version of software updates when available.

SECTION 12: Electronic Communications System Usage Policy

All users of Judiciary information systems must acknowledge and comply with the Electronic Communications System Usage Policy and are bound to modifications as posted to the Employee Handbook.

SECTION 13: Data Loss Prevention

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use, data in motion and data at rest. DLP controls are based on policy and include classifying sensitive data, discovering that data across an enterprise, enforcing controls and reporting and auditing to ensure policy compliance. A comprehensive DLP solution should include the following controls:

- Use network monitoring tools to analyze outbound traffic looking for anomalies which may include large file transfers, long-time persistent connections, connections at regular repeated intervals, unusual protocols and ports in use, and possibly the presence of certain keywords in the data traversing the network perimeter. For any unauthorized port connection made on the JIS network, the system will be designed to reroute the traffic to an unrouteable network for further investigation and analysis. Tools will be used to detect and deactivate unused network ports.
- Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting appropriate personnel.
- Use outbound proxies to monitor and control all information leaving the Judiciary.
- Use secure, authenticated, or encrypted mechanisms to move confidential data between untrusted networks.
- Confidential data stored on removable and easily transported storage media such as USB thumb or flash drives and CDs/DVDs must be secured.
  All electronic media decommissioned or disposed of by Judiciary entities must be destroyed in accordance with AOC and District Courts of Maryland processes and procedures.

SECTION 14: Software Licenses and Use

- Unless specifically approved by the Chief Information Officer, a user's personal or a contractor's business PC or laptop shall not have Judiciary proprietary or licensed software installed and shall not be used to process or transmit proprietary or confidential information.
- Only Judiciary owned and authorized computer software is to be used on Judiciary owned machines. Users are not authorized to download or install software on a Judiciary owned PC or laptop.
- All users of Judiciary information systems must comply with copyright laws.

SECTION 15: Wireless Security

Policies and Procedures supporting the use of wireless technology used in the JIS managed network shall:

- Establish a process for documenting all wireless access points.
- Ensure proper security mechanisms are in place to prevent the theft, alteration or misuse of access points, introduction of rogue devices or access to the Judiciary network.
- Restrict hardware to Wi-Fi certified devices that are configured to use the latest security features available.
- Change default administrator credentials.
- Change default SNMP strings if used, otherwise disable SNMP.
- Change default SSID.
- Deploy secure access point management protocols and disable telnet.
- Strategically place and configure access points to minimize SSID broadcast exposure beyond the physical perimeter of the building.
- Require wireless users to provide unique authentication over encrypted channels, with a minimum encryption level of WPA2.