Minimum Security Standards

DRAFT 12/4/15

Requirements or Control	Currently Meets	Explanation	Plan & Timeline
Computer Room Physical & Environmental Controls			
All server and network equipment is located in a controlled-access area(s) that have physical restrictions on entry, to supporting staff only. If a controlled-access area is not available, equipment is enclosed in locked racks.			
Unauthorized employees or vendors are logged and escorted in controlled-access area(s).			
Controlled-access areas display no signage indicating they are a computer facility.			
A UPS (uninterrupted power supply) having sufficient battery time to prevent data loss is in place and functional.			
Smoke, water, fire, and high/low temperature detection devices are operational in any unmanned controlled access areas.			
Escallation procedures are in place in the event of an issue in the controlled-access area.			
User Authentication & Access Controls			
Access to computing and network resources is only granted upon written request through an incident management software tool and approved by the manager or supervisor of the requestor.			
Individual UserIDs all conform to a standard format. Generic UserIDs are only used in the case of "Service Accounts/programmatic access."			

Minimum Security Standards

DRAFT 12/4/15

Requirements or Control	Currently Meets	Explanation	Plan & Timeline
Passwords have a minimum length of 8 characters and contain a minimum of 2 alpha characters and 2 numeric characters. Admin. passwords should also include 1 special character in it.			
User IDs are deactivated after a 30-day period of inactivity and all associated privileges revoked. IDs are reviewed for deletion after 60 days.			
Third-party vendors are not given external access privileges to Judicial Branch servers and/or networks without a business-requested, justifiable need. Privileges are enabled only for the time period required to accomplish the approved tasks or the contract time period, whichever is shorter.			
User passwords are changed at least once every 60 days. Service accounts' (non-user) passwords are changed at least once every 6 months, whenever the system allows.			
Passwords are never stored in readable form in locations where unauthorized persons could discover them. Sharing passwords between users is prohibited.			
Initial passwords, or passwords that have been reset by an admin, are changed to a unique password at first login.			
To prevent password guessing, passwords are limited to 3 incorrect attempts prior to being disabled from use.			
Every password on a system is changed at the time of the next log-in whenever system security has been compromised or there is a convincing reason to believe it has been compromised.			

Minimum Security Standards

DRAFT 12/4/15

Requirements or Control	Currently Meets	Explanation	Plan & Timeline
Authoritative site contacts inform the AOC Customer Support Center of the termination of any AJIN user prior to or immediately upon termination.			
System privileges granted to users are reevaluated by local management periodically and in response to changes in job role. When informed by management, system admins promptly revoke all privileges no longer needed by users.			
Termination of an employee with "Admin" system access results in immediate password change to all systems.			
Upon termination of an employee, the immediate manager determines the custodian of the employee's files and/or the appropriate methods to be used for disposal. Unless instructed otherwise, 4 weeks after termination, all files held in that user's personal folders are purged.			
AJIN Access from Outside the Domain			
No local subdomains, web servers, new local area networks, backdoor connections to existing local area networks, or other equipment used for data communication are attached to AJIN without specific approval from AOC Network Services.			
VPN connections are controlled solely by AOC Network Services. Remote connections that do not use approved products and go through approved processes are prohibited.			

Minimum Security Standards

DRAFT 12/4/15

Requirements or Control	Currently Meets	Explanation	Plan & Timeline
VPN connections to AJIN domains and/or server systems pass through an access control point /firewall before users employing these connections reach a log-in banner.			
User-based communication access between AJIN users and external resource environments occurs only by direct access through an AOC firewall. This may also include a one-way domain trust for user authenication.			
Programmatic access into the AJIN network is permitted only via AJIN edge firewalls, VPN, or IBM MQ IPT front end.			
All server and client devices accessing the AJIN network have up-to-date anti-virus protection on them. Anti-virus programs are protected against user access and never disabled.			
Computing and Network Devices within AJIN			
Confidential or restricted information is appropriately classified at its source.			
All "confidential " or "restricted" information transmitted over any communication network other than AJIN is only sent in an encrypted form.			
All Web-based devices and printers communicating outside of the AJIN network only do so using TLS and have an authenticated certificate installed.			
All AJIN domain servers and workstations have approved anti-virus screening software enabled on their computers at all times. Users can not disable or deactivate this software.			

Minimum Security Standards

DRAFT 12/4/15

Requirements or Control	Currently Meets	Explanation	Plan & Timeline
All downloaded files from non-Judicial-Branch sources are screened with virus detection software prior to being opened/saved/executed.			
Computing and Network Devices within AJIN			
All PCs employ a locking screen saver program which requires a password to access. Timeout is set to no longer than 10 minutes of inactivity.			
User shares and general shared folders do not default to read, write, and execute for anonymous users. Shares are restricted to specific domain Users and/or Groups.			
Web sites that contains sexually explicit racist, violent, or other potentially offensive material are blocked using third-party lists, updated frequently.			
To the extent that systems software permits, computer and communications systems handling Judicial Branch information log all user connections.			
User access logs are retained for at least 3 months and secured such that they cannot be modified and can be read only by authorized persons.			
All network intrusion detection is done through AOC Network Services. Detection logs are backed up and retained for a 30-day window.			
All computer and network devices are maintained with the latest vendor-provided security and firmware updates available for the specific O/S.			

Minimum Security Standards

DRAFT 12/4/15

Requirements or Control	Currently Meets	Explanation	Plan & Timeline
Security audit scans by the AOC of all computing devices in all domains contained within the AJIN network occur once a quarter. Reports are distributed to local administration staff. Defined vulnerabilities are remediated immediately.			
Computing and Network Devices within AJIN			
Notification of any new server or printer being added to the AJIN network is communicated to AOC Infrastructure Operations via Remedy ticket prior to being commissioned.			
Local court adminisrators are responsible to ensure that local applications loaded on AOC-supported desktop/laptop systems are patched and that no security vulnerabilities exist.			
No device residing on the AJIN network has dual access to a non-AJIN network without being approved and configured by the AOC.			
All network equipment used to grant access onto the AJIN network is the responsibility of the AOC Network Services. This includes, but is not limited to, routers, switches, and access points.			
Any use of network monitoring tools on the AJIN network is approved by AOC Network Services prior to use. Data capturing tools are prohibited on AJIN.			
The laws for copyrights, patents, trademarks, and the like are enforced as stated in the Arizona Judicial Department Electronic Communication Policy. Copying of pirated or bootleg software is strictly prohibited.			