JIS General Policies

With Comments

Last Revised by the JISC: October 24, 2014

Table of Contents

Authority 1
Scope 1

Authority

RCW 2.68.010 gives the JISC the authority to "determine all matters pertaining to the delivery of services available from the judicial information system." JISC Rule 1 provides for AOC to operate the Judicial Information System (JIS) under the direction of the JISC and with the approval of the Supreme Court pursuant to RCW 2.56. RCW 2.68.050 directs the courts, through the JISC, to provide electronic access to judicial information.

Scope

These policies apply to all persons, organizations, or agencies that operate, manage, or use the portfolio of IT products and services provided by AOC.

~~Judicial Information System General Policies~~

~~*With Comments Annotations*~~

1. EQUIPMENT

1.1 General

~~*Amended by the Judicial Information System Committee on August 14, 2009.*~~

COMMENT

Historically the JIS provided some end user equipment as each trial court system (SCOMIS, DISCIS, JUVIS) was implemented. The amount of equipment distributed depended on the available funds. With the

implementation of the IP network and the need to replace "dumb" terminals with personal computers, the JIS initiated the first equipment replacement plan in 1996.

1.1.1 The Judicial Information System (JIS) is the system owned and maintained by the Administrative Office of the Courts (AOC). A JIS court is a court that uses the JIS to process its cases from filing to closure. A non-JIS court is a court that contributes information electronically to the statewide JIS database.

1.1.2 Subject to available funding, the AOC provides end-user equipment including personal computers and printers for court personnel and county clerks in JIS and non-JIS courts. The AOC does not provide equipment for users other than courts and county clerks.

COMMENT

The JIS is funded for equipment in the Judicial Branch and County Clerks (who are the clerks of the superior courts) only.

1.1.3 Subject to legislative funding, the number of JIS computers provided to courts is calculated at up to 75 percent (75%) of the FTEs from the most recent staffing report published by AOC~~The JIS standard is one personal computer per employee whose job requires one~~; one report printer per six administrative or clerical FTEs with a minimum of one report printer per court or clerk's office; for limited jurisdiction courts, one receipt printer per cashier with a minimum of one receipt printer per court or clerk's office; and for superior court clerks one cash drawer, slip printer and receipt printer per cashier with a minimum of one cash drawer, slip printer and receipt printer per court.

COMMENT

The policy of JIS funding up to 75% of personal computers, based on FTE counts, was decided by the JIS Executive Committee on April 18, 2006, based on the principle of a need for local-state cooperation to share responsibility for equipment that is used for JIS applications and for local applications and tasks. However, all JIS equipment replacement is limited by legislative funding. ~~principle of one personal computer per employee and the standards for printers and receipting equipment were established in a motion adopted by the JIS Committee on June 21, 1996. However, because of limited budgets, equipment supplied by the JIS has been limited to one for one replacement of existing end user equipment.~~

1.1.4 Equipment is provided to the users defined in sub-sections 1.1.1 and 1.1.2 for the purpose of enabling judicial officers, clerks, court administrators, and clerks' and court administrators' staff to access and update the JIS, to do legal

research, or for other court business purposes. JIS-owned equipment not used for court business purposes shall be returned to the AOC.

1.2 Replacement of Personal Computers, Printers, and Related Equipment

1.2.1 Basic Rule

Subject to legislative funding, the JIS provides a one for one replacement of JIS supplied and JIS funded equipment on a five year cycle.

COMMENT

The five year standard was established with the first replacement cycle in 1996. ~~The other branches of state government also use a five year cycle.~~

1.2.2 Reimbursement for Locally Purchased Personal Computers

COMMENT

Because of the nature of the JIS network architecture, which often includes local jurisdictions' area networks, it is often desirable for local jurisdictions to buy and maintain equipment themselves. Therefore, the JIS provides for local purchase of JIS-funded court and county clerk equipment under reimbursement plans. This allows the local jurisdictions to maintain consistent equipment standards and simplifies maintenance.

1.2.2.1 If a local court or county clerk's office prefers to purchase its replacement computer equipment rather than use that supplied by the JIS, the JIS will reimburse the court or county clerk for the actual cost of the equipment or a specified amount based on current market prices per device, whichever is less.

1.2.2.2 The JIS will not provide maintenance coverage for locally purchased equipment covered by a reimbursement plan.

1.2.2.3 Computer equipment purchased under a reimbursement plan must meet current published JIS minimum standards.

COMMENT

In order to help ensure the efficient delivery of the JIS to the courts and county clerks, the JIS maintains, through the AOC, standards for personal computers. The standards include minimum requirements for processor speed, RAM capacity, hard drives, CD-ROM drives, display, sound, and web browser.

1.2.2.4 Contractual ~~Inter-agency~~ agreements ~~Local Cooperative Agreements (ICAs)~~ will be used for reimbursements.

COMMENT

The JIS Committee approved the use of reimbursements and Inter-Local Cooperative Agreements to implement them on June 21, 1996. The Interlocal Cooperation Act, Chapter 39.34 RCW, provides for and governs the use of such agreements.

1.2.3 Retention of Old Equipment

Courts and county clerks may keep old JIS-owned equipment after it has been replaced. State inventory tags must be removed from the equipment and replaced equipment becomes locally owned. Repair and maintenance of this equipment is the responsibility of the court or county clerk.

In some instances, older computers may not be able to support up-to-date security controls or requirements. ~~This is due to an inability to upgrade the chipsets or firmware, in order to mitigate newer threats.~~ In such instances, where older hardware is incompatible with current security measures, AOC may disallow or block connection from obsolete devices.

~~The JIS does not allow courts or county clerks to keep old JIS-owned equipment after it has been replaced.~~

~~*The retention of old equipment presents several regulatory maintenance, and resource problems. The JIS does not have funds budgeted to maintain such equipment. Moreover, as equipment ages it becomes more difficult to maintain and maintenance services and parts become less available. Because of State of Washington General Administration regulations for disposal of used assets, it is not practicable to simply transfer ownership to a local court or county clerk that would take over the maintenance responsibility. In addition, keeping such equipment in service would require that the JIS expend funds to add capacity to the switching equipment the JIS supplies for network connections.*~~

1.2.4 New Judges and Employees

1.2.4.1 Equipment for court and county clerk staff who were added after a replacement cycle will be provided in the next cycle, provided sufficient funds are available.

1.2.4.2 Equipment for new judges will be provided at the time judgeships are funded and filled~~created~~, provided sufficient funds are available.

1.3 Locally Owned Equipment

1.3.1 Courts and county clerks may use locally owned equipment ~~personal computers~~ to access and use the JIS.

1.3.2 ~~An~~ IBM-compatible equipment ~~PC~~ is required for courts and county clerks to connect~~ions~~ to and use ~~of the~~ JIS.

1.4 Security and Care of JIS Owned Equipment

1.4.1 Courts and county clerks must exercise due care (1) to ensure that JIS-owned equipment is installed in locations that are secure, and (2) in their use of JIS-owned equipment. The JIS insures equipment against loss and theft. Damage due to negligence is the responsibility of the court or county clerk.

1.4.2 When connecting personal computers and printers to electrical power, courts and county clerks must use surge protectors that meet JIS standards.

1.5 Maintenance of Equipment; Service Calls

1.5.1 The JIS provides maintenance coverage for any JIS-owned equipment (subject to the exceptions identified in these policies).

1.5.2 The JIS pays repair costs for broken JIS-owned equipment and for the resolution of problems related to the JIS provided software when the problem is determined to be caused by defective hardware, or an act of nature (fire, storm damage, etc.). Costs for repairs related to negligence (e.g., damage resulting from spillage, falls, misuse, etc.) are the responsibility of the court or county clerk. Repair costs include parts, travel, and labor costs.

1.5.3 AOC Customer Services handles service calls from courts for JIS-owned hardware. Customer Services will only accept calls from authorized callers (those authorized by court or county clerk management), Site Coordinators, Administrators, or County Clerks.

1.5.4 AOC Customer Services handles service calls from courts and county clerks for court and county clerk-owned equipment when the court or county clerk has a maintenance contract with the same maintenance vendor as the JIS (currently Cascade Computer Maintenance). In such cases, CCM will directly bill the court or county clerk for charges resulting from such calls.

COMMENT

Customer Services recommends that courts and county clerks discuss all hardware issues with their local Information Services departments, if they have one, prior to calling Customer Services for a service call. This will alleviate unnecessary service calls and subsequent billings at the court or county clerk's expense for local network settings that are handled at a local level.

1.6 Upgrades of JIS Owned Equipment

1.6.1 Unauthorized peripherals (monitors, keyboards, speakers, etc.) may not be attached to JIS-owned personal computers.

COMMENT

The attachment of such peripherals negates the PC warranty and complicates problem resolution and service provisions.

1.6.2 Unauthorized components (additional hard drives, memory, etc.) may not be installed in JIS-owned personal computers.

COMMENT

The addition of such components negates the PC warranty and complicates problem resolution and service provisions.

1.7 Equipment for Judges

COMMENT

Policies for judges' equipment were established by the JIS Equipment Subcommittee on October 13, 1998 and reviewed by the JIS Committee on October 23, 1998. The allocation policy for municipal court judges was established by the JIS Equipment Subcommittee on November 19, 1999. In the original distribution to municipal court judges, the standard was that the court have a minimum annual domestic violence case load of 48 cases, based on 1998 numbers.

1.7.1 Each superior and district court judge and each ~~full-time~~ commissioner employed .5 FTE or more is eligible for one personal computer and one laser printer. ~~Full-time is defined as a .5 or more full time equivalent.~~

1.7.2 Judicial officers in Judicial Districts are eligible for one printer per courtroom at each court location.

1.7.3 Municipal court judges who are either full-time, or whose courts have a substantial domestic violence caseload, are eligible for one personal computer and one laser printer.

1.7.4 Judges' personal computers are eligible for reimbursement contracts~~ICAs~~.

2 NETWORKS & CONNECTIVITY

2.1 General

2.1.1 The JIS will provide each court and county clerk with a network connection, including such required equipment as routers and switches, to the JIS systems and data base.

COMMENT

Historically, the JIS has provided the telecommunications network used to connect the JIS to the courts. The formal policy was approved in a motion adopted by the JIS Committee on June 21, 1996. Originally, the network consisted of dedicated circuits and the proprietary IBM SNA protocol. With the implementation of the TCP/IP protocol it became feasible to use shared network resources, including the state's backbone, the InterGovernmental Network, county and city area networks.

2.1.2 Other criminal justice users may use court network connections, provided no additional costs are incurred to enable their use.

Shared networks provide benefits both to users (more services are available) and to the JIS (costs are reduced).

2.1.3 Wherever possible, the JIS will use the state's InterGovernmental Network (IGN) to connect to local courts. In such cases, local criminal justice agencies which use the JIS may also use the IGN to connect, provided JIS security requirements are met. In the cases where the connection to a local court uses the IGN, the JIS pays the "anchor tenant" portion of the ~~DIS~~ charges. In such cases, counties or cities will be responsible for ~~DIS~~ local government connection charges.

COMMENT

State agencies are~~DIS~~ charge~~d~~s ~~both~~ ~~state agencies~~ to ~~which~~ use the IGN ~~to deliver~~ production applications ("anchor tenants") and local governments are charged for the connection to IGN. Local charges are usually paid by the county or city government, not the courts or county clerks, and cover usage by all local government agencies.

2.1.4 The JIS will not provide support for the portion of the network connection that involves a local network (i.e., between a router [InterGovernmental Network or JIS supplied] and a ~~hub or~~ switch used to connect devices in a court or county clerk's office).

COMMENT

This policy was approved in a motion adopted by the JIS Committee on June 21, 1996.

2.2 Network Security

COMMENT

Court and county clerk, and to some extent, local prosecutor and law enforcement, connections to the JIS are based on the Internet Protocol (IP) over shared networks or, in some cases, dedicated frame relay circuits. This section describes the requirements and architecture for connection to the JIS

over an IP network using the state InterGovernmental Network, a county or city area network, a dedicated frame relay circuit, a local Ethernet, or a combination. These network architecture requirements are designed to enforce security by isolating JIS traffic from parts of networks where end user devices for non-criminal justice users are attached. In this scheme, courts, county clerks, law enforcement, and prosecutors are considered trusted and may be located in places on the network where JIS traffic is transmitted. Other local agency users ~~are not trusted and~~ may not access the local network ~~from the portions~~ connections dedicated to criminal justice.

2.2.1 The IP address assigned to a JIS workstation identifies the workstation and serves to distinguish between authorized and unauthorized workstations (or between secured and unsecured, or trusted and untrusted workstations).

2.2.2 When connections are made, courts and county clerks already connected to county or city networks shall retain the IP addresses they have obtained from their counties or cities. Courts and county clerks planning to connect to county or city networks, as well as to JIS, shall obtain subnet addresses from their county or city. AOC will provide a VPN connection in instances where the county or city does not have sufficient resources. ~~, except that, where the county or city does not have sufficient IP addresses, the JIS will provide IP addresses for personal computers and printers used by courts or county clerks to access the JIS. A two week turnaround is required when requesting IP addresses from AOC.~~

2.2.3 If the court or county clerk has no external connections to a county or city network, AOC will provide network resources via a VPN tunnel ~~IP addresses will be provided by AOC~~.

2.2.4 IP addresses shall be statically assigned to printers used to connect to the JIS. Workstation addresses may be dynamic where approved by AOC technical staff. A network address translator (NAT) may also be used where approved by AOC technical staff.

2.2.5 ~~When a county or city network is used to connect a court to the JIS and the network is not switched, the local network shall be segmented to isolate JIS traffic.~~

2.2.6 A county or city IP segment connected to the JIS network may consist of court, county, clerk, prosecutor, and/or law enforcement agency workstations. Workstations used by other agencies may not be connected to such segments.

2.2.7 Users that are logged onto a JIS resource, by use of a RACF ID and password, may not use unauthorized applications or services that creates a remote connection to another computer or network. Doing so would make available the same access to data and privileges the logged on JIS user has,

to unknown and potentially untrusted individuals. Tools used by technical support personnel to remotely manage computers on their networks are not subject to this requirement. These types of remote sessions take place within the boundaries of the trusted network, and do not create "external" connections.

~~JIS users may not connect computers that are members of the JIS Network to other networks via remote access software or hardware. Remote access applications, designed for this purpose, my not be installed on JIS computers. Modems may not be incorporated into or attached to any personal computer, regardless of whether the JIS or the court owns it, which connects to the JIS via a static IP connection.~~

COMMENT

Products like PCAnywhere and Logmein install a product on a personal computer (PC) which continually ping a server. Users can connect to the server and create a tunnel to the PC with minimal credentials. Using a VPN to connect to the county network, and then using Microsoft Remote Desktop Connection, is acceptable, as that utilizes a secure tunnel and full credentials.

~~Remote access software or hardware~~ ~~Dial-up facilities (using software such as PC Anywhere)~~ ~~presents a significant risk to the JIS network and database. They potentially allow third parties to access a JIS user's PC and thereby the JIS itself.~~

~~**2.2.8** Modem pools may be connected to a local network used by JIS workstations on a case by case basis with the approval of the AOC. The local jurisdiction shall provide to the AOC the details of the security protection for such modem pools. AOC shall review such security schemes and approve the use of such modem pools only if the security is adequate.~~

~~Modem pools attached to local networks present similar significant risks as modems incorporated into or attached to personal computers. However, because modem pools may be secured against such risks, their use is permitted subject to a security review.~~

2.2.8 Wireless Networks

COMMENT

Because of the high risk of unauthorized access, this policy is designed to govern the use of wireless LANs for JIS access, except for public access subscribers. A wireless LAN could circumvent the network security architecture prescribed in this section. Unless there is stringent local network security that specifically addresses wireless LANs, it is easy to install an unauthorized wireless LAN and attach it to a local network without detection.

Without proper security, it is also easy for unauthorized users to connect through a wireless LAN even if it is authorized.

2.2.8.1 The AOC, at its discretion, may approve connections from personal computers on wireless networks, or on networks that include wireless segments provided the agency responsible for the wireless network certifies in writing that it has done the following:

2.2.8.1.1 Complied with AOC standards for wireless networks.

2.2.8.1.2 Establish, document, and communicate wireless access security practices within the agency.

2.2.8.1.3 Implement a program to perform ~~an~~ audits at ~~on a~~ regular intervals ~~basis~~ for the purpose of locating and removing ~~in order to locate any~~ rogue wireless devices.

2.2.8.2 Agencies approved access from wireless networks or networks including wireless segments shall certify at least once every two years to the AOC, in writing, that they are adhering to these wireless policies and applicable AOC technical standards. AOC may routinely monitor for unauthorized wireless devices, by use of network Host Intrusion Detection Systems (HIDS), and physical wireless surveys.

2.2.8.3 If the AOC implements a wireless network, it must comply with the requirements of this section.

2.2.8.4 Public access subscribers are not subject to policies on wireless networks.

COMMENT

Public access subscribers do not have access to confidential data and use Secure Sockets Layer (SSL) for encryption. In addition, public access subscribers will have to pay for any unauthorized transactions. It is up to them to control and police their networks.

~~**2.3 Dial Up Access**~~

~~**2.3.1** On request, judicial officers may be enabled for dial in access to the JIS.~~

3 SOFTWARE

3.1 Software on JIS Owned Equipment

3.1.1 The JIS will supply the operating system and a TN3270 terminal emulation program for all JIS-owned personal computers.

COMMENT

For PCs supplied by the JIS, the JIS provides software essential to operating the PC and obtaining JIS services. The JIS provides a Microsoft Windows operating system, which includes the Internet Explorer web browser.

Because JIS legacy systems use 3270 terminal protocols, a TN3270 client is required to access them in the IP environment. ~~The TN3270 client the JIS currently provides is Seagull Software Bluezone.~~

The JIS ~~provides a limited number of licenses for Brio (see Section 3.1.3, below) but~~ does not provide anti-virus ~~checkers~~ or other software. Because of the need to constantly update such products ~~virus checkers~~, it is not feasible for the JIS to supply them. All courts and county clerks, including those which use JIS-owned equipment, are strongly advised to acquire and install anti-virus software ~~checkers~~.

3.1.2 The JIS will supply a TN3270 terminal emulation program for any personal computer owned by a local court or county clerk and used to perform court work on the JIS.

COMMENT

For court and county clerk-owned PCs, the JIS provides the software essential to obtaining JIS services. However, because the operating system is so closely associated with the PC, it is the responsibility of the PC owner to provide it, including the web browser. The JIS does not provide virus checkers or other software.

~~**3.1.3 Brio**~~

~~*Allocations of Brio licenses are based on funds available to buy and maintain the licenses.*~~

~~**3.1.3.1** Superior Courts are allocated three copies per court -- two copies for the clerk, one for the administrator. The clerk and administrator may also agree on a different distribution.~~

~~**3.1.3.2** Juvenile Courts are allocated three copies per court.~~

~~**3.1.3.3** Courts of Limited Jurisdiction are allocated one copy per court and, if additional copies are available, may obtain them on a first-come first-served basis.~~

3.1.3 Court-Provided Software

3.1.3.1 Courts and county clerks may install software (e.g., word processors, spreadsheets, etc.), provided they hold a valid license for it, on JIS-owned

personal computers, except for those personal computers used for the Judicial Receipting System (JRS).

3.1.3.2 Courts and county clerks may replace the operating system on JIS-owned personal computers with a system that meets the current JIS standard.

COMMENT

The AOC recommends that courts and county clerks not replace the operating system on JIS-owned PCs. The current standard requires a Microsoft Windows operating system. The AOC encourages the use of reimbursement funds during equipment replacement projects if other than standard AOC-issued operating systems are required.

3.1.3.3 Courts and county clerks are responsible for ~~bear the risk of~~ any problems associated with ~~any~~ locally installed software, and therefore, are liable for any maintenance costs related to incidents or outages caused by such products ~~it~~.

3.1.3.4 JIS users may not use software that allows remote viewing of, control of, or access to any personal computer that connects to the JIS. Courts and county clerks may allow their county and city information services providers to remote control PCs when required for technical support, and the user is notified that the remote control is happening.

COMMENT

Programs such as GoToMyPC that allow remote access of a personal computer present a significant security risk because of the potential ease of access by third parties when a user's PC is enabled for remote access. At the same time user technical support services need to be able to use programs such as Microsoft SMF for PC and software maintenance and troubleshooting.

3.2 Software Requirements for Use of the JIS

3.2.1 Windows users' browsers must be maintained at a version not older than the oldest version supported by the vendor ~~Internet Explorer 5.5 or higher~~. AOC may set more specific standards for browsers, applications and plugins, based on known usability and security issues.

COMMENT

For example, if a user has Internet Explorer (IE) version 5.5, and Microsoft no longer provides updates for IE versions below version 9.0, the browser must be upgraded at local cost to at least version 9.0.

3.2.2 Cookies must be enabled in browser properties.

4 SECURITY

4.1 Access Rules

4.1.1 Access To The JIS

Except for public access programs such as JIS-Link and the Washington Courts (www.courts.wa.gov) Internet website, access to the JIS computer systems is restricted to authorized personnel who have been assigned a JIS user account. For courts and county clerks, JIS Site Coordinators, under the direction of the county clerk or court administrator, are authorized to assign JIS accounts to individual court or county clerk employees. Such assignments shall be based on each employee's work responsibilities and business need for access and other privileges.

4.1.2 Update Privileges

Information in the JIS database may be updated by court and county clerks' office personnel only. All others shall be restricted to read-only access.

4.1.3 Court User IDs

Courts and county clerks may assign user IDs to their employees only. Only court employees may have court level access and update privileges associated with court user ids.

4.1.4 User Account Deactivation

It is the responsibility of the site coordinator to deactivate an employee's user account (user id and password) upon termination of the employee's employment. Such deactivation must be done at the time the employee last leaves the court or clerk's office premises, regardless of when the employee actually leaves the payroll.

4.1.5 User Responsibilities

Users shall respect the privacy of other JIS network users and the integrity of their data. Users shall not seek information on other users; obtain copies of or modify files, other data, or passwords belonging to other users; or represent themselves as another user.

4.1.6 Password Locked Screensavers

Password locked screensavers shall be used on all personal computers connected to the JIS from the courts, or connected to the AOC network and must be set to initiate the screensaver no more than 15 minutes after the last use.

COMMENT

This control is necessary to support guidance set forth in section 4.4.1.3 of this

policy. JIS connected computers will be configured in such a way that court users cannot change or disable this setting.

4.1.6.1 Password Locked Screensavers provide a critical safeguard and may not be disabled. However, in certain instances where business practices are sufficiently impacted, the 15 minute time limit may be extended. The AOC ISD Director will consider such extension requests on a case-by-case basis, and make the final determination after performing a thorough business impact and security analysis.

4.1.7 Reporting Misuse

Any JIS user who suspects misuse of his/her user account or workstation shall report such incidents to the JIS Site Coordinator. Site Coordinators shall report such incidents to AOC Customer Services.

4.1.8 Confidentiality Agreements

An employee of a court or county clerk's office may access the JIS only if he or she has signed a confidentiality agreement in a form approved by the AOC. Employees of courts or county clerks' offices shall review the confidentiality agreement annually.

4.1.9 Access b~~B~~y Vendors, Contractors, and Staff of Local Information Technology Departments

Vendors, contractors, and staff of local information technology departments may be granted security privileges for access to non-public data in the JIS if such access is needed in order to develop or maintain an information system for a court or the AOC. Such access shall be governed by written agreements between the AOC, the court or county clerk, and the vendor, contractor, or local information technology department. Such contracts shall require the employees of the vendor, contractor, or local information technology department to sign a confidentiality agreement, and for the court or county clerk to keep the signed copies and to certify to the AOC that such agreements have been executed.

4.2 Passwords

COMMENT

Passwords are an essential part of the JIS security. This section contains basic rules for passwords based on standards developed by the National Institute of Standards and Technology (NIST) and which are generally accepted best practices. Passwords are often the most vulnerable component ~~part~~ of an organization's security strategy ~~scheme~~. Because they are subject to many kinds of attacks and are dependent on user behavior, strong

passwords, that are changed frequently, are required. See, for example, such sources as NIST's Implementation Checklists; NIST Special Publication 800-53, Recommended Security Controls for Federal Information System; Federal Information Processing Standards Publication 112, Standard for Password Usage; and Gartner's Best Practices for Managing Passwords.

4.2.1 User access to the JIS and to judicial branch networks is regulated through the use of user id's and passwords. User id's and passwords shall be assigned to individuals only. Group, or "generic" user accounts and credentials are not authorized for this purpose.

4.2.2 Each user is responsible for maintaining the confidentiality of his or her password and shall not reveal the password to anyone.

4.2.3 User id's and passwords shall not be shared.

4.2.4 Passwords shall not be recorded on paper or maintained in clear text files.

4.2.5 The JIS requires the use of passwords which have the following characteristics:

4.2.5.1 Passwords must be exactly of 8 characters long.

4.2.5.2 Passwords must contain at least one upper case letter, one lower case letter, and one numeral. Passwords may contain special characters that are compatible, as determined by AOC ~~alphabetic and one numeric character~~.

4.2.5.3 Passwords must not contain the user's login name, or any part of their full name.

4.2.6 JIS security software shall enforce the requirements for passwords and the following business rules:

4.2.6.1 Passwords must be changed at least every 90 days.

4.2.6.2 The last 10 passwords used by an individual must be unique.

4.2.6.3 After five attempts to log in with an incorrect password, the user id must be revoked and the user must place a call to AOC Customer Services to reinstate the account.

4.3 Control of Public Access Terminals

4.3.1 Public access terminals connected directly to the JIS must meet the access rules established by AOC. Public Access terminals connected to city or county networks and/or the IGN must meet the rules established for those networks as well as AOC.

4.3.2 Public access to the JIS from a court may be provided only from a PC dedicated to public access and set up for that purpose. Such PCs must meet standards for public access terminals established by the AOC.

4.3.3 Courts and county clerks shall employ only public access user ids (designed for public access) when logging into the JIS personal computers used as public access terminals. Other court or county clerk user ids may not be used on public access PCs. ~~All p~~Public access logons shall have ~~be~~ read only privileges.

4.4 Access to the AOC Network

COMMENT

The "AOC Network" is the group of interconnected Local Area Networks (LANs) used by the Supreme Court, Court of Appeals and AOC. It is the home of the JIS mainframe and servers. This policy section applies to all appellate court and AOC employees, contractors, consultants, temporary employees, and anyone else, including those affiliated with third parties, who accesses the AOC network. This section applies to access to the AOC network from personal computers on the network itself and to implementations of remote access that allow direct access to the AOC network from outside the AOC network. The Infrastructure Department has responsibility for monitoring access and for establishing procedures and technical standards. Requests for access to the AOC network must be made by submission to AOC Customer Services of a completed Network Access Request (NAR) form. The AOC Network Access Request form will denote authorization levels, which will vary depending on applicant and access purpose.

4.4.1. General Policy on Access to the AOC Network

COMMENT

These policy sections apply to all access and requests to access the AOC network regardless of whether the access is from a personal computer connected directly to the network or from a personal computer connected to the network from ~~at~~ a remote location ~~not on the network~~.

4.4.1.1. Approved AOC and appellate court employees and authorized third parties (consultants, vendors, etc.), when authorized by an appropriate authority, may be granted access to the AOC network:

- from personal computers directly connected to the network; and/or
- from personal computers using a secure remote access connection.

4.4.1.2. AOC employees may be authorized by their immediate manager, department manager, or the AOC Employee Services Section. Third parties under contract to the Administrative Office of the Courts may be authorized by the manager responsible for the contract. Supreme Court employees or third parties under contract to the Supreme Court may be authorized by a justice or department head. Court of Appeals employees or third parties under contract to the Court of Appeals may be authorized by a judge or the clerk of their division.

4.4.1.3. Access is controlled by user id and password authentication. Each user must have a unique account. Shared accounts are not permitted. The password must comply with Section 4.2 of this policy.

Once a user has successfully logged onto a computer connected to the JIS, they may not leave that computer unattended without first logging off or locking the terminal. This action is necessary to avoid unauthorized access to JIS data and preserve the integrity of security logs.

4.4.1.4. All users are subject to audit of their use of the network.

4.4.1.5. AOC network access for non-AOC or appellate court personnel is limited to the network resources to which they need access.

~~**4.4.1.6.**~~ Users of the AOC network may use only AOC supplied or approved services to send and receive email. AOC mail servers provide numerous security mechanisms to combat malicious attachments and phishing attempts, and avoid unauthorized access to JIS and user information. ~~To prevent the infiltration of viruses and other malicious software the AOC shall block access to other email services.~~

4.4.2. Secure Remote Access to the AOC Network

COMMENT

These policy sections regulate remote access from personal computers not directly connected to the AOC network. The typical user is an employee connecting from home. ***By using remote access technology with personal equipment, users must understand that their machines are a de facto extension of the AOC network, and as such are subject to the same rules and regulations that apply to AOC owned equipment. This means their machines must be configured to comply with all relevant security policies and requirements.***

Secure remote access is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing any required software. Secure remote access is an IP (Internet Protocol) only resource. Other protocols are not supported.

4.4.2.1 Remote access users will be automatically disconnected from the AOC network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Devices or applications, designed to generate false activity, in order to keep the connection from timing out, ~~Artificial network processes~~ may not be used ~~to keep the connection open~~.

4.4.2.2 Violation of this policy may result in termination of service. Contracts with individuals and organizations who need secure remote access shall specify that the AOC or other judicial branch contracting entity may terminate the contract in the event of a violation of this policy.

4.4.2.3 If any suspicious activity is detected, the AOC may terminate a user's access without notice and, at its discretion, not reinstate access until the issue has been identified and resolved.

4.4.2.4 Users must comply with applicable AOC Infrastructure polices, procedures and technical standards.

4.4.2.5 Users requesting secure remote access must certify that they have read and understand this policy and applicable AOC Infrastructure polices, procedures and technical standards.

4.4.2.6 It is the responsibility of the employee or organization with secure remote access privileges to ensure that unauthorized users are not allowed access to AOC secure network.

4.4.2.7 All remote access gateways will be set up and managed by AOC Network Operations staff. User created gateways are not permitted on the secured network.

4.4.2.8 All computers remotely connected to AOC secure network must use up-to-date virus-scanning software with the most recent virus definitions. Computers or devices connected to AOC may require local installation of AOC supplied client software to monitor and enforce AOC security policies and practices.

4.4.2.9 The remote access user must keep the security patches up to date for the operating system of any personal computer used to connect to the AOC network ~~up to date~~. Computers or devices connected to AOC may require local installation of AOC supplied client software to monitor and enforce AOC security policies and practices.

4.4.2.10 Users of computers that are not the property of AOC must configure the equipment to comply with this policy and AOC Infrastructure security policy and technical standards.

4.4.2.11 Only AOC approved applications and procedures may be used to remotely access the AOC network ~~by remote access users~~.

4.4.2.12 Users of remote access services are responsible for the procurement and cost associated with acquiring basic Internet connectivity and for resolving any associated service issues.

4.5 Data Security

COMMENT

The JIS contains sensitive and confidential information, including personally identifiable information (PII). PII is any information about an individual maintained by an agency that can distinguish or trace an individual's identity, or can create a link to an individual. Examples may include date of birth, place of birth, social security number, address, mother's maiden name, financial account numbers, credit card numbers, medical information and educational information. To ensure the security of sensitive and confidential information in JIS, personally identifiable information must only be contained in the appropriate part of the system. Personally identifiable information in inappropriate areas of JIS, such as text fields, are vulnerable to access by those not authorized to view the information.

4.5.1 No JIS users shall enter social security numbers into the Judicial Information System. Employer identification numbers may be entered for the purpose of reporting interest earned on accounts held in trust pending the outcome of a case.

4.5.2 The Judicial Information System will not contain social security numbers. Employer identification numbers are permissible for the purpose of reporting interest earned on accounts held in trust pending the outcome of a case.

4.5.3 Personally identifiable information in JIS shall only be in the fields identified for that information. Personally identifiable information shall not be contained in any other part of the JIS.

5 ON-LINE AND OTHER SERVICES

5.1 Access to Westlaw

The JIS provides no cost access for judicial officers and to court, county clerks' offices and judicial branch employees who need to do legal research to a standard set of Westlaw databases.

5.2 Email

5.2.1 Email for Judicial Officers

COMMENT

These policies on email for judges were established by the JIS Equipment Subcommittee on October 13, 1998 and reviewed by the JIS Committee on October 23, 1998.

5.2.1.1 The JIS provides email addresses and email client software to judicial officers who do not have county or city addresses.

5.2.1.2 The JIS provides email addresses to judicial officers who have county or city email services, and who are concerned about local policies that give control of email to the executive branch, or where local security of email is not adequate.

5.2.2 Listserv~~ers~~

5.2.2.1 The JIS provides a listserv~~er~~ to facilitate sending and receiving email to designated groups, such as judicial branch and association committees.

~~**5.3 The Internet**~~

~~**5.3.1** The JIS does not provide Internet access for trial courts or county clerks.~~

~~**5.3.2** Judges may access the JIS via the Internet.~~

5.3 The Extranet (Inside.Courts.Wa.Gov)

5.3.1 Access to the extranet is restricted to judicial officers, county clerks and their staffs, court employees, and other employees of the judicial branch.

5.3.2 Access to the extranet may be granted by the AOC Information Services Director on a temporary basis to city and county information technology department employees, or others in local government if it is necessary to perform services for the judicial branch or a court.

5.4 Data Warehouses~~ and Direct Access to the JIS Database~~

COMMENT

The data warehouse is a central repository of court data. Court data is uploaded nightly to the JIS data warehouse.

5.4.1 In all cases governed by Section 5.5, access will be appropriate to the user's case level security.

5.4.2 Courts and county clerks will be granted access to the JIS data warehouse using AOC supplied and maintained query software.

5.4.3 Requests for access to additional data elements must be submitted to AOC Customer Services.

~~**5.4.1** Courts and county clerks will be granted access using AOC supplied query software to data warehouses containing JIS data.~~

~~*Currently, the query software for the data warehouse is Brio Insight. The policy on the allocation of JIS-funded Brio licenses is in Section 3.1.3. The existing data warehouse contains limited jurisdiction court data only. Therefore, county clerks have been enabled to have direct access as provided in Section 5.5.2.*~~

~~**5.4.2** A court's or clerk's information technology staff, a local jurisdiction's information technology department, a vendor, or contractor may be granted direct access to the JIS database if the court or clerk approves the request in conjunction with services provided to the court or clerk to develop or maintain an information system.~~

~~*Currently, direct access shall be through the use of ODBC (open data base connectivity). In the future, direct access to the production database will likely be replaced by access to an operational data store, which would be a duplicate of the production database.*~~

~~*The policy on Access By Vendors, Contractors and Staff of Local Information Technology Departments is in Section 4.1.9.*~~

~~**5.4.3** In all cases governed by Section 5.5, access will be restricted to the data related to cases filed in the local jurisdiction.~~

~~**5.4.4** Data elements available via direct access will be controlled by AOC using database views. A court or county clerk who wants access to additional data must submit a change request.~~

~~**5.4.5** The AOC shall provide a standard form contract for direct access arrangements that involve non-court entities such as local information technology departments, contractors, or vendors. Such contracts shall specify requirements for the protection and non-disclosure of confidential information as provided in Section 4.1.9.~~

6 USE OF CUSTOMER SERVICES

6.1 AOC Customer Services provides assistance to courts, county clerks, criminal justice and other public agency users~~, and JIS-Link general subscribers~~. It

does not provide assistance to third-party clients of JIS-Link subscribers and does not provide phone training in the JIS-Link application.

6.2 Only designated users may place calls to Customer Services. Designated users include judicial officers~~, including judges,~~ county clerks, court administrators, and site coordinators, and court staff who are designated by their administrator as authorized callers.~~may place calls to Customer Services~~.

7 IMPLEMENTATION OF COURTS AS JIS USERS

COMMENT

This section reflects the notion that the JIS cannot provide resources unless its budget contains funding for them. New municipal courts are typically established outside of state budget cycles. The JIS does periodically plan and budget for implementation of existing non-JIS courts.

7.1 Newly Established Municipal Courts

7.1.1 The JIS will not supply end-user equipment (printers or personal computers).

7.1.2 Courts must acquire and use equipment which meets current JIS standards.

7.1.3 The JIS will provide equipment or reimbursement in future replacement cycles.

7.1.4 The JIS will provide network connections as described under “networking,” above.

7.1.5 The JIS will provide training and implementation services to the extent resources are available.

7.1.6 The JIS will provide limited telephone assistance on equipment and implementation issues.

7.2 Existing Courts Which Join JIS

7.2.1 The JIS will provide a full set of end user equipment at no cost to courts which join during AOC programs to add courts.

7.2.2 The JIS will provide a single set of equipment (PC and printer) at no cost to Courts which join at other times.

7.2.3 Equipment courts acquire and use must meet current JIS standards.

7.2.4 The JIS will provide equipment or reimbursement in future replacement cycles based on current allocation rules.

7.2.5 The JIS will provide network connections as described under “networking,” above.

8 NEW COURT OR COUNTY CLERK FACILITIES

COMMENT

This policy section reflects the notion that relocation decisions are made locally and therefore the local court should be responsible for their impacts.

Relocation requires coordination and advance planning with the AOC. The AOC requires eight weeks in advance notice so that appropriate connectivity can be established.

8.1 The JIS will not pay for the cost to relocate equipment and wiring.

8.2 The JIS will provide standard category 5 wire to courts needing such wire.

8.3 The JIS will be responsible for any required relocation of network connections.

8.4 The JIS does not provide equipment for additional new locations of existing JIS courts.

9 SUPPLIES

COMMENT

Historically, the JIS has supplied standard form paper and ribbons for printers dedicated to printing reports from JIS. The JIS has not supplied or paid for forms unique to a court, or for supplies related to laser printers which may be used for non-JIS purposes.

9.1 The JIS will supply standard form printer paper and ribbons for impact and dot matrix printers in the courts.

9.2 The JIS does not supply or cover the cost of special forms.

9.3 The JIS will not supply or cover the cost of toner, paper, or photo conductors for either court owned or JIS-owned laser printers.

9.4 The JIS will not replace batteries in laptops supplied to the courts.

10 JIS APPLICATIONS

10.1 Requests for JIS Application Service~~Change Management~~

10.1.1 ~~Change~~ Routine requests involving application access, use, security, or data quality must ~~will~~ be submitted through AOC Customer Services ~~categorized according to the following scheme~~ and will be managed by AOC.

~~Request Category~~	~~Time to Respond~~	~~Time to Resolve~~
~~Emergency Application Access (Problems with a database, communication lines, system releases, and other activity that impair the use and access to any judicial application and resource)~~	~~Level 1 (1 to 48 hours)~~	~~Level 1 (1 to 48 hours)~~
~~Security (Identified or possible breaches in authorized access to the system by court staff or other application users, changes to increase or decrease authorized access to any judicial application and resource)~~	~~Level 1 (1 to 48 hours)~~	~~Level 2 (1 to 72 hours)~~
~~Data Quality (Problems caused by corrupt, inconsistent, or erroneous data entered by application user or errors caused by application)~~	~~Level 3 (24 hours to 1 week)~~	~~Level 4 (2 weeks to 1 month)~~
~~Business Policy and Practices (Identifies policies and practices that degrade efficiency in judicial processes and the operation of an application)~~	~~Level 4 (2 weeks to 1 month)~~	~~Level 5 (Up to 2 months or more)~~
~~Application Enhancements (New or enhanced features and functionality to the judicial application)~~	~~Level 2 (1 to 72 hours)~~	~~Level 5 (Up to 2 months or more)~~
~~Legislative Mandates (Changes required by law)~~	~~Level 1 (1 to 48 hours)~~	~~Level 5 (Up to 2 months or more)~~

10.1.2 ~~Level 1-3 requests are generally handled by AOC working with courts and involves no committee participation. Level 4 and 5 requests require AOC to coordinate with courts, committees, and other external agencies.~~

10.1.2 Requests involving ~~business policy and practices,~~ application enhancements or replacement, legislative or court rule mandates, and non-emergency data requests ~~quality problems~~ must be submitted through the IT Governance Portal ~~to the JIS Advisory Committee~~ and follow the IT Governance Framework and JIS IT Governance Policy, approved by the JISC ~~JIS Change Request Guidelines~~.

10.2 Alternative ~~Custom~~ ~~Local~~ Systems, Interfaces, Reports and Services

10.2.1 The JIS provides case management automation to courts and maintains a statewide network providing access to the JIS database. To implement this, the JISC selects and provides equipment and services. The JISC plans for, implements, and supports case management applications that provide baseline functionality to the courts of Washington State. The JISC acknowledges that some courts desire alternative services and/or applications to meet their local needs. Courts that implement alternative applications or services are responsible for the costs of acquiring, developing, implementing, and maintaining such systems.

For those courts that do not use the statewide vendor solution as chosen by the Judicial Information Systems Committee, Judicial Information Systems account funds may not be allocated for (a) the costs to meet the data collection and exchange standards developed by the Administrative Office of the Courts and the Judicial Information Systems Committee, and (b) the costs to acquire, develop, implement or maintain alternative court case management systems.

10.2.2~~1~~ Access to JIS systems will only be through AOC-supported data exchange methods. Courts may create their own custom user interfaces, reports or services (including data exchanges) consistent with the standard JIS application programming interfaces (API's) for business services or the JIS enterprise data warehouse.

10.2.3~~2~~ Custom extensions developed to meet local needs do not require JIS Committee approval and will receive no JIS support.