JIS General Policies

With Comments

Last Revised by the JISC: October 24, 2014

Table of Contents

Authority 1
Scope 1
1. EQUIPMENT 2
2. NETWORKS & CONNECTIVITY 6
3. SOFTWARE 9
4. SECURITY 11
5. ON-LINE AND OTHER SERVICES 18
6. USE OF CUSTOMER SERVICES 20
7. IMPLEMENTATION OF COURTS AS JIS USERS 20
8. NEW COURT OR COUNTY CLERK FACILITIES 21
9. SUPPLIES 21
10. JIS APPLICATIONS 22

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.

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

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 charges. In such cases, counties or cities will be responsible for local government connection charges.

COMMENT

State agencies are charged to use the IGN 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 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 may not access the local network 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.

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.

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 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.

2.2.6 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.

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.

~~2.2.7 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.*~~

~~**2.2.7.1** 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:~~

~~**2.2.7.1.1** Complied with AOC standards for wireless networks.~~

~~**2.2.7.1.2** Establish, document, and communicate wireless access security practices within the agency.~~

~~**2.2.7.1.3** Implement a program to perform audits at regular intervals for the purpose of locating and removing rogue wireless devices.~~

~~**2.2.7.2** 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.~~

~~**2.2.7.3** If the AOC implements a wireless network, it must comply with the requirements of this section.~~

~~**2.2.7.4** 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.*~~

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 JIS does not provide anti-virus or other software. Because of the need to constantly update such products, 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.

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 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 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.

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 AOC is responsible for and will ensure that the JIS application(s) support new Microsoft Windows operating systems and Internet Explorer browser versions within six (6) months of general release. Subsequently, once operating systems and browser versions are no longer supported by the manufacturer, support for that version by the JIS application will cease.

3.2.2 Windows users' browsers must be maintained at a version supported by the JIS applications ~~not older than the oldest version supported by the vendor~~s. 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.