



Arizona Judicial Information Network (AJIN) Security Manual

Addendum H: LAN Design Standards to Connect to AJIN

Scope:

How a network is physically configured to transmit information from one point to another is based on an engineering design structure that grants or restricts access to information. To ensure the security of the information and to assist in understanding how access is granted or restricted the following rules have been established for Class 1 and Class 2 courts.

A. Class 1 and Class 2 courts

1. Connections to the Internet will be protected by a firewall.
2. Connections to a county or city network will be protected by a firewall.
3. Connections from a court to AJIN will utilize Triple DES security when dictated by the applications (e.g. Tax Intercept Program (TIP) and Atlas)
4. Servers and network equipment should be physically located in a controlled area limited to operational and identified vendor support personnel.
5. Personnel will use user_id and password as a minimum for authentication.
6. Network and computer systems will have a system access log that records all attempts to access the system.
7. Virus scanning software will be installed on all servers and desktop.
8. Modems should not be installed on desktops.
9. Modems on servers should be set for dialing out only.
10. Desktops, network printers and servers should have static IP addresses.
11. IP address management
12. DHCP

B. Class 1 courts only

1. Connections are administered by the AOC.
2. Network equipment will be administered by the AOC.
3. Servers will have a windows server operating system.
4. Servers in the AOC domain will be administered by the AOC.
5. IP addressing will be controlled by the AOC.
6. E-mail and domain login access will be controlled by the AOC.

C. External Agencies

1. Connections to the Internet will be protected by a firewall.
2. Connections to AJIN will be protected by a firewall.
3. Connections from AJIN will utilize Triple DES security when dictated by the applications (e.g. Tax Intercept Program (TIP) and Atlas)
4. Virus scanning software will be installed on all servers and desktop.
5. IP address



Arizona Judicial Information Network (AJIN) Security Manual

Addendum I: List of Class 1 sites

Site	Speed	Class
Ajo Justice	56k	1
Apache Junction Justice	T-1	1
Apache Junction Municipal	56k	1
Apache Junction Probation	56k	1
Apache Juvenile Probation	56k	1
Apache Superior	T-1	1
Avondale Municipal	56k	1
Bagdad Justice	56k	1
Benson Justice and Probation	T-1	1
Bisbee Justice	56k	1
Bisbee Municipal	56k	1
Bowie Justice	56k	1
Buckeye Municipal	56k	1
Bullhead City Justice	3mb	1
Bullhead City Municipal	3mb	1
Bullhead City Probation	56k	1
Camp Verde Municipal	56k	1
Carefree Municipal	56k	1
Casa Grande Justice	T-1	1
Casa Grande Juvenile Probation	T-1	1
Casa Grande Municipal	T-1	1
Cave Creek Municipal	56k	1
Chambers Juvenile Probation	56k	1
Chinle Justice	56k	1
Chino Valley Municipal	56k	1
Clarkdale/Jerome Municipal	56k	1
Clifton Municipal	56k	1
Cochise County Attorney Office	56k	1
Cochise Juvenile Probation	T-1	1
Cochise Superior	T-1	1
Coconino Juvenile Probation	T-1	1
Coconino Superior	T-1	1
Coolidge Municipal	56k	1
Cottonwood Alternative Center	56k	1
Cottonwood County Complex	T-1	1
Douglas Justice	56k	1
Douglas Municipal	56k	1
Douglas Probation	56k	1
Duncan Justice and Municipal	56k	1



Arizona Judicial Information Network (AJIN) Security Manual

Duncan Justice and Municipal	3mb	1
East Santa Cruz/Sonoita	56k	1
El Mirage Municipal	56k	1
Eloy Justice	T-1	1
Eloy Municipal	56k	1
Flagstaff Extended	56k	1
Flagstaff Municipal	T-1	1
Florence Justice	56k	1
Florence Municipal	56k	1
Fountain Hills Municipal	56k	1
Fredonia Justice and Municipal	56k	1
Gila Bend Municipal	56k	1
Gila Superior	T-1	1
Glendale Municipal	T-1	1
Goodyear Municipal	56k	1
Graham Juvenile Probation	3mb	1
Graham Superior	3mb	1
Green Valley Justice	56k	1
Greenlee Juvenile Probation	3mb	1
Greenlee Superior	56k	1
Greenlee Superior	3mb	1
Guadalupe Municipal	56k	1
Hayden Municipal	56k	1
Holbrook Downtown Probation	T-1	1
Huachuca Municipal	56k	1
Kayenta Justice	56k	1
Kearny Municipal	56k	1
Kingman Justice	3mb	1
Kingman Municipal	3mb	1
La Paz Superior	T-1	1
Lake Havasu City Complex	3mb	1
Lake Havasu City Probation	56k	1
Litchfield Municipal	56k	1
Mammoth Municipal	56k	1
Marana Municipal	56k	1
Maricopa Justice	56k	1
Mayer Justice	56k	1
MCAP consultants	T-1	1
Moccasin Justice	56k	1
Mohave Juvenile Detention	2mb	1
Mohave Juvenile Probation	2mb	1
Mohave Superior	T-1	1
Navajo Juvenile Detention	56k	1
Navajo Juvenile Probation	56k	1
Navajo Superior	T-1	1



Arizona Judicial Information Network (AJIN) Security Manual

Nogales Municipal	56k	1
Open Inn Coconino Office	56k	1
Oracle Justice	56k	1
Oro Valley Municipal	56k	1
Page Justice and Municipal	56k	1
Page Juvenile Probation	56k	1
Page Library (Court Help)	56k	1
Parker Municipal	56k	1
Patagonia Municipal	56k	1
Payson Justice and Municipal	T-1	1
Payson Juvenile Probation	56k	1
Peoria Municipal	T-1	1
Pima Justice	3mb	1
Pima Juvenile Probation	T-1	1
Pinal Conciliation Court	56k	1
Pinal County Attorney Office	56k	1
Pinal Detention	56k	1
Pinal Juvenile Probation	56k	1
Pinal Superior	T-1	1
Pinetop Probation	56k	1
Pinetop/Lakeside Justice	56k	1
Prescott Valley Municipal	T-1	1
Puerco Justice	56k	1
Quartzsite Justice	56k	1
Quartzsite Municipal	56k	1
Round Valley Justice	56k	1
Round Valley Juvenile Probation	56k	1
Safford Justice and Municipal	3mb	1
Sahuarita Municipal	56k	1
Salome Justice	56k	1
San Luis Municipal	56k	1
Santa Cruz Juvenile Detention	56k	1
Santa Cruz Probation Annex	T-1	1
Santa Cruz Superior	T-1	1
Scottsdale Municipal	56k	1
Sedona municipal	56k	1
Seligman Justice	56k	1
Showlow Justice	56k	1
Showlow Juvenile Probation	56k	1
Showlow Municipal	56k	1
Sierra Vista Justice and Municipal	T-1	1
Sierra Vista Service Center	T-1	1
Snowflake Justice and Municipal	56k	1
Snowflake Probation Office	56k	1



Arizona Judicial Information Network (AJIN) Security Manual

Somerton Justice and Municipal	56k	1
South Tucson Municipal	56k	1
Superior Municipal	56k	1
Surprise Municipal	56k	1
Thatcher Municipal	3mb	1
Tolleson Municipal	56k	1
Tombstone Municipal	56k	1
Verde Valley Justice	T-1	1
Wellton Justice and Municipal	56k	1
Wickenburg Municipal	56k	1
Wilcox Justice and Probation	56k	1
Wilcox Municipal	56k	1
Williams Justice and Municipal	56k	1
Winkleman Municipal	56k	1
Winkleman Probation	56k	1
Winslow Justice and Probation	56k	1
Winslow Municipal	56k	1
Yarnell Justice	56k	1
Yavapai Juvenile Probation	T-1	1
Yavapai Superior	T-1	1
Youngtown Municipal	56k	1
Yuma Adult Probation	56k	1
Yuma Judicial Assistance	56k	1
Yuma Juvenile Probation	T-1	1
Yuma Municipal	T-1	1
Yuma Superior	T-1	1



Arizona Judicial Information Network (AJIN) Security Manual

Addendum J: List of Class 2 sites

Site	Speed	Class
Maricopa County	T-1	2
Pima Superior	T-1	2
State Bar	T-1	2
Tucson City	T-1	2
Mesa Municipal	T-1	2
Tempe Municipal	T-1	2
Phoenix Municipal	T-1	2
Chandler Municipal	No connection	2
Gilbert Municipal	No connection	2
Paradise Municipal	No connection	2
Queen Creek Municipal	No connection	2



Arizona Judicial Information Network (AJIN) Security Manual

Addendum K: Minimum Recommended Hardware Supported on AJIN

COMPUTERS			
Manufacturer	Equipment Type	Configuration	Operating System
COMPAQ	Desktop Evo D510	Pentium IV, 1.8 GHZ Processor, 256 MB Internal Memory, 20G Hard Drive, 48 X CD-ROM Drive, 1.44 Floppy Drive, 10/100 NIC	Windows 2000
COMPAQ	Monitor V7550	17"	N/A
COMPAQ	Laptop Evo N600C	Pentium III, 1.2 GHZ Processor, 256 MB Internal Memory, 30G Hard Drive, DVD/CDRW Drive, 1.44 Floppy Drive, 10/100 NIC, 56K modem	Windows 2000

PERIPHERIALS

Manufacturer	Equipment Type	Configuration	Operating System
Hewlett-Packard	Laserjet 4100N	25 pages per minute, 32MB memory	NA

SERVERS

COMPAQ	ProLiant DL380	Pentium III, 1GHZ Processor, 1GB Internal Memory, (3) 18GB Hard Drive, 10/100 NIC, 20GB DLT Tape Drive and UPS	NT 4.0
IBM	Pseries 640	2- way 375MHZ, 516MB, 18.2 GB internal drive, (4) 36.4GB external Drive, 10/100 NIC, 20GB 8mm tape Drive and UPS	AIX 4.3

NETWORK

Manufacturer	Equipment Type	Model Numbers	Number of Users
IBM	Router	2210- 1U8, 12E, 24E, 2212	12, 64, 200, 500
CISCO	Router	2501, 2621, 3640, 7206	64, 200, 300, 500
CISCO	Firewall	PIX1000, 506, 515, 525	300, 120, 200, 500
CISCO	Switch	1924, 2916, 2924, 3524, 5000, 6000	24, 100, 200, 300, 300, 500
Kentrox	CSU/DSU	1000(T1), 651(T1)	Determined by Router
Paradyne	CSU/DSU	3510(56K), 3160(T1)	Determined by Router
CISCO	Wireless Access	Aeronet 350(LEAP,MIC,WEP128,ACS)	10
CISCO	RAS Servers	2620, AS5300(Crypto Key, ACS)	8, 128
FSONA	Optics Bridge	622-M(Gigabit)	N/A
Wi-Lan	Wireless Bridge	HP45-24(4 Mbps)	N/A
CSPEC	Wireless Bridge	OVERLAN 100 (100Mbps)	N/A
CSPEC	Wireless Bridge	RF-10 (2Mbps) No new installs	N/A
CISCO	Access Control Sys	ACS 3.X	N/A
KRONE	Cabling	Cat5e or better	N/A



Arizona Judicial Information Network (AJIN) Security Manual

Addendum L: Internet Web Site Categories Blocked by AJIN

CATEGORIES BLOCKED BY WEBSense

CATEGORY	DIRECTORY	HOURS
Adult		
	<i>Adult Content</i>	Always
	<i>Nudity</i>	Always
	<i>Sex</i>	Always
	<i>Lingerie&Swimsuit</i>	Business
Entertainment		
	<i>MP3</i>	Always
	<i>Gambling</i>	Always
	<i>Illegal/Questionable</i>	Always
	<i>Games</i>	Business
Information Technology		
	<i>Hacking</i>	Always
	<i>Proxy Avoidance Systems</i>	Always
	<i>Url Translation Sites</i>	Always
Internet Communications		
	<i>Web Chat</i>	Always
Sports		
	<i>Tasteless</i>	Always
	<i>User Defined</i>	Always
Special Lifestyles		
	<i>Personnel Dating</i>	Business
	<i>Special Events</i>	Business
	<i>All Other Categories are open at all hours.</i>	
	<i>Business Hours</i>	6:00am - 7:00pm
	<i>Off Hours</i>	7:00pm - 6:00am



Arizona Judicial Information Network (AJIN) Security Manual

Addendum M: File-Attachments “Blocked” in AJIN E-mail

As many of you may already be aware of, there is rapid evolution of viruses and development of new viruses. Due to these factors Anti-Virus software and their customers are always slightly “behind the curve” on updates for virus detection. Even though we are notified of a new virus and the characteristics, the detection software is not provided for several days. One safeguard that we are using as an organization is to block certain file types that are sent via email. Blocking these file types prevents an executable file from reaching a person’s mailbox, whether it contains a virus or not. Although it may at times be convenient to have the ability to send these file types, there are much safer alternatives. The risk of losing or crippling the mail systems for the AOC and all the Courts on AJIN for hours or even days due to a virus infection far outweighs the convenience of sending executable attachments.

To help protect the organization from such a virus infection the following file types are blocked as attachments for the AJIN email system:

File Extension	Description
.BAT	Batch file, a basic text file containing DOS system commands that will activate
.CHM	Compiled HTML help file for Windows (An updated help file)
.COM	Command File – A small version of an executable file (program)
.EML	Email File
.EXE	Executable File (program)
.GZ	A Unix system Zip or compressed file
.HTA	An HTML or web-based application
.LNK	Shortcut Icon – The actual picture (icon) that represents the shortcut to an object in Windows, i.e. X
.PIF	Program information file. Descriptor used to run a DOS program in Windows
.SCR	Screen Saver file
.VBS	Visual Basic (Programming Language) Script file



Arizona Judicial Information Network (AJIN) Security Manual

Addendum N: RECORDS RESTRICTED BY ARIZONA LAW

- Abortion proceedings involving a pregnant minor (ARS § 36-2152)
- Adoption records (ARS §§ 8-120, -121)
- Audit files maintained by Auditor General (ARS § 41-1279.05)
- Automobile accident reports (ARS § 28-667)
- Banking Branch records (ARS § 6-129)
- Birth certificates and information pertaining to births out-of-wedlock in the state system of vital records (ARS § 36-340(C) & 36-346(A)(5))
- Board of Medical Examiners records (ARS § 32-1451.01(C))
- Business information in air pollution investigations (ARS § 49-432(D))
- Business information in fuel use tax reports (ARS § 28-5935)
- Child abuse and neglect records (ARS § 8-807)
- Child custody hearing records (ARS § 25-407)
- Child welfare and placement records (ARS §§ 8-541, -542, -546.03)
- Civil rights investigations (ARS § 41-1481(B))
- Cleared arrest records (ARS § 13-4051)
- Commerce Branch records (ARS §§ 41-1505.06(D), -1505.07(K))
- Conciliation Court records (ARS § 25-381.16)
- Consumer fraud information provided to Attorney General (ARS § 44-1525)
- Corrections Branch records (ARS § 31-221)
- County Recorder records of peace officers (ARS § 11-483)
- Criminal history record information (ARS § 41-1750)
- Death records used to correct voter registration (ARS § 16-165)
- Economic Security Branch records (ARS § 41-1959)
- Educational records (ARS § 15-828)
- Employing unit reports for DES (ARS § 23-722)
- Evaluations of certified teachers (ARS § 15-537)
- Executive session minutes (ARS §§ 38-431.03(B), 39-121)
- Fingerprint records of deceased persons (ARS § 11-593(F))
- Geothermal wells data (ARS § 27-653)
- Health Services Branch records (ARS §§ 36-107, -340, -404, -509, -714(B)(1))
- HIV-related confidential information held by insurance companies (ARS § 20-448.01)
- Hospital records (ARS §§ 12-2281, 36-509)
- Indictments (and accompanying unexecuted arrest warrants) (ARS § 13-2813)
- Insurance holding company business records (ARS § 20-481.21)
- Law enforcement officers' license plate records (ARS § 28-454)
- Medical malpractice claims and actions reported by insurers to BOMEX (ARS 32 § 1855.02)
- Medical records (ARS § 12-2292)



Arizona Judicial Information Network (AJIN) Security Manual

- **Non-profit corporate disclosure of records and other matters (ARS § 15-1638)**
- **Ombudsman-citizens aide investigation (ARS § 41-1378)**
- **Physician-patient privilege (ARS § 12-2235)**
- **Plaintiff's address in a petition for an injunction against harassment (if requested by plaintiff) (ARS § 12-1809)**
- **Plaintiff's address in an order of protection (if requested by plaintiff) (ARS § 13-3602)**
- **Psychologist - client communications (ARS § 32-2085)**
- **Revenue Branch records relating to tax information (ARS §§ 42-2002, -2054)**
- **Search warrant and supporting records (ARS § 13-3918)**
- **Unemployment insurance tax reports (ARS § 23-722)**
- **Unlawful employment practices reports (ARS § 41-1482)**
- **Victims' right to privacy (ARS § 13-4434)**
- **Wiretapping records (ARS § 13-3011)**
- **Victim's identity in juvenile court records (ARS § 8-208)**

STATE COURT RULES

- **Case file and administrative court records, certain materials (Supreme Court Rule 123)**
- **Indictments issued by a state grand jury (Ariz. R. Crim. Pro. 12.26)**
- **Discovery materials in a criminal trial (Ariz. R. Crim. Pro. 15.4)**
- **Jurors' home and business addresses and phone numbers (Ariz. R. Civ. Pro. 47(a); Ariz. R. Crim. Pro. 18.3)**
- **Victims' personal identifying information (Ariz. R. Crim. Pro. 39(b)(10))**



Arizona Judicial Information Network (AJIN) Security Manual

GLOSSARY

Access control: A system to restrict the activities of users and processes based on the need-to-know.

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation; generally used to refer to the process for performing encryption.

Approving Authority: The judge, clerk of court, administrator, or their designated to supervisor authorized users.

Badge reader: A device which reads badges and interconnects with a physical access control system.

Booting: The process of initializing a computer system from a turned-off state.

Bridge: A device which interconnects networks or that otherwise allows networking circuits to be connected.

Closed Information: A designation for information, that is considered "Closed" or "Confidential", according to Rule 123 which refers to records, that members of the public may not inspect, obtain copies of, or otherwise have access to unless authorized by law. Personal financial documents containing social security, credit card, debit card, or financial account numbers or credit reports of an individual, when collected by the court for administrative purposes are also considered closed. (See restrictive information).

Chief Information Officer: The AOC Director in charge of all information processing in the Judicial Branch.

Cipher lock: A device that requires the entry of passwords at doors and which provides physical access control over a room or building.

Compliance statement: A document used to obtain a promise from a computer user that such user will abide by system policies and procedures.

Confidential information: A designation for information, that is considered "Closed" or "Confidential", according to Rule 123 which refers to records, that members of the public may not inspect, obtain copies of, or otherwise have access to unless authorized by law. Personal financial documents containing social security, credit card, debit card, or financial account numbers or credit reports of an individual, when collected by the court for administrative purposes are also considered closed. (See restricted information).



Arizona Judicial Information Network (AJIN) Security Manual

Critical information: Any information essential to Judicial Branch's business activities, the destruction, modification, or unavailability of which would cause serious disruption to Judicial Branch's business.

Cryptographic challenge/response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then, transformed using an encryption process and a response is returned to the connected computer system.

Default file permission: Access control file privileges (read, write, execute, etc.) granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password issued when a new user-ID is issued, or an initial password provided by a computer vendor when hardware/software is first delivered.

Dynamic password: A password which changes each time a user logs-into a computer system.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time-stamping, and other security objectives.

End-user: A user who employs computers to support Judicial Branch business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process achieved by user-IDs and fixed passwords (see hand-held tokens and dynamic passwords).

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security check (such as providing a password).

Front-end telecommunications processor: A small computer used to handle communications interfacing (polling, multiplexing, error detection, etc.) for another computer.

Gateway: A computer system used to link networks which can restrict the flow of information and which employs some access control method.

Hand-held token: A commercial dynamic password system which employs a smart card to generate one-time passwords that is different for each session.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the timeframes that these types of information must be kept.

Isolated computer: A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.



Arizona Judicial Information Network (AJIN) Security Manual

Log-in banner: The initial message presented to a user when he or she first makes connection with a computer.

Log-in script: A set of stored commands which can log a user into a computer automatically.

Master copies of software: Copies of software which are retained in an archive and which are not used for normal business activities.

Server system: Any computer which can support more than one user simultaneously.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password reset: The assignment of another (temporary) password when a user forgets or loses his/her password.

Password-based access control: Software which relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user-ID: A user-ID which has been granted the ability to perform special activities, such as shut down a multi-user system.

Restricted information: Particularly information, the disclosure of which is expected to damage the Judicial Branch's customer relations or public image (see confidential information).

Router: A device that interconnects networks using different layers of the Open Systems Interconnection (OSI) Reference Model.

Screen blanker: See screen saver.

Screen saver: A computer program that automatically blanks the screen of a computer monitor or CRT after a certain period of no activity.

Security patch: A software program used to remedy a security or other problem (commonly applied to operating systems).

Sensitive information: Any information, the disclosure of which could damage Judicial Branch or its business associates.



Arizona Judicial Information Network (AJIN) Security Manual

Shared password: A password known by and/or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges allowing the involved user or process to perform activities which are not normally granted to other users.

Suspending a user-ID: The process of revoking the privileges associated with a user-ID.

Systems administrator: A designated individual who has special privileges on a server system, and who looks after security and other administrative matters.

Users: Refers to all court officials and employees who are users of the Arizona Judicial Information Network and also includes any non-court persons who are authorized users.

User-IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Judicial Branch or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.