

Iowa Judicial Branch
Information Systems Acceptable Use Policy
March 24, 2006

1.0 Overview

Information Security Officer's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Iowa Judicial Branch established culture of openness, trust and integrity. Information Security Officer is committed to protecting Iowa Judicial Branch's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Iowa Judicial Branch. These systems are to be used for business purposes in serving the interests of the Iowa Judicial Branch, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Iowa Judicial Branch employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Iowa Judicial Branch. These rules are in place to protect the employee and Iowa Judicial Branch. Inappropriate use exposes Iowa Judicial Branch to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Iowa Judicial Branch, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Iowa Judicial Branch.

4.0 Policy

4.1 General Use and Ownership

1. While Iowa Judicial Branch's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on Judicial Branch systems remains the property of Iowa Judicial Branch. Because of the need to protect Iowa Judicial Branch's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Iowa Judicial Branch.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. Information Security Officer recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Information Security Officer's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Information Security Officer Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within Iowa Judicial Branch may monitor equipment, systems and network traffic at any time, per Information Security Officer Audit Policy.
5. Iowa Judicial Branch reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by Iowa Judicial Branch confidentiality guidelines, details of which can be found in Human Resources policies. Examples

- of confidential information include but are not limited to: Judicial Branch private, Judicial Branch strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords and user level passwords should be changed monthly. Microsoft AD Administration account must be changed quarterly.
 3. All PCs, laptops and workstations should be **secured** with a password-protected screensaver with the automatic activation feature set to department guidelines, or by logging-off (control-alt-delete for Win2K and XP users) when the host will be unattended.
 4. Use encryption of information in compliance with Information Security Officer's Acceptable Encryption Use policy.
 5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
 6. Postings by employees from a Iowa Judicial Branch email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Iowa Judicial Branch, unless posting is in the course of business duties.
 7. All hosts used by the employee that are connected to the Iowa Judicial Branch Internet/Intranet/Extranet, whether owned by the employee or Iowa Judicial Branch, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
 8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Iowa Judicial Branch authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Iowa Judicial Branch-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Iowa Judicial Branch.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Iowa Judicial Branch or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an Iowa Judicial Branch computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any Iowa Judicial Branch account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Information Security Officer is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Iowa Judicial Branch employees to parties outside Iowa Judicial Branch.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Iowa Judicial Branch's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Iowa Judicial Branch or connected via Iowa Judicial Branch's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term Definition

Spam Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

4/17/2006 1:33 PM

Changed 4.2(2) to meet password policy guidelines.
Changed 4.2(3) to defer screen saver timeout to departmental guidelines.

Iowa Judicial Branch Remote Access Policy March 28, 2006

1.0 Purpose

The purpose of this policy is to define standards for connecting to Iowa Judicial Branch's network from any host. These standards are designed to minimize the potential exposure to Iowa Judicial Branch from damages which may result from unauthorized use of Iowa Judicial Branch resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Iowa Judicial Branch internal systems, etc.

2.0 Scope

This policy applies to all Iowa Judicial Branch employees, contractors, vendors and agents with an Iowa Judicial Branch-owned or personally-owned computer or workstation used to connect to the Iowa Judicial Branch network. This policy applies to remote access connections used to do work on behalf of Iowa Judicial Branch, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of Iowa Judicial Branch employees, contractors, vendors and agents with remote access privileges to Iowa Judicial Branch's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Iowa Judicial Branch.
2. General access to the Internet for recreational use by immediate household members through the Iowa Judicial Branch Network on personal computers is not permitted.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Iowa Judicial Branch's network:
 - a. *Acceptable Encryption Policy*
 - b. *Virtual Private Network (VPN) Policy*
 - c. *Wireless Communications Policy*
 - d. *Acceptable Use Policy*

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Iowa Judicial Branch employee provide their login or email password to anyone, not even family members.
3. Iowa Judicial Branch employees and contractors with remote access privileges must ensure that their Iowa Judicial Branch-owned or personal computer or workstation, which is remotely connected to the Iowa Judicial Branch network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Iowa Judicial Branch employees and contractors with remote access privileges to the Iowa Judicial Branch network must not use non-Iowa Judicial Branch email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Iowa Judicial Branch business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Iowa Judicial Branch network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.

8. Non-standard hardware configurations must be approved by Remote Access Services, and ISO must approve security configurations for access to hardware.
9. All hosts that are connected to Iowa Judicial Branch internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to Iowa Judicial Branch's networks must meet the requirements of Iowa Judicial Branch-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Iowa Judicial Branch production network must obtain prior approval from Remote Access Services and ISO.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Judicial Branch network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on an Iowa Judicial Branch-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Iowa Judicial Branch and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64 kbps (aggregate 128kbps) and 1 D channel for signaling info.

Remote Access	Any access to Iowa Judicial Branch's corporate network through a non-Iowa Judicial Branch controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-Iowa Judicial Branch network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Iowa Judicial Branch's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.
DLCI	A data link connection identifier (DLCI) is a channel number which is attached to data frames to tell the network how to route the data. A 13-bit field that defines the destination address of a packet. The address is local on a link-by-link basis.

6.0 Revision History

4/17/2006 1:23 PM	Added definition for DLCI. Deleted 3.1(4) which discussed access option which was too broad.
-------------------	---

Iowa Judicial Branch Server Security Policy March 28, 2006

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Iowa Judicial Branch. Effective implementation of this policy will minimize unauthorized access to Iowa Judicial Branch proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by Iowa Judicial Branch, and to servers registered under any Iowa Judicial Branch-owned internal network domain.

This policy is specifically for equipment on the internal Iowa Judicial Branch network. For secure configuration of equipment external to Iowa Judicial Branch on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at Iowa Judicial Branch must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review by Information Security Officer.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
 - Server contact(s) and location, and a backup contact
 - Hardware and Operating System/Version
 - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved Iowa Judicial Branch IT guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root/admin when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - All security related logs will be kept online for a minimum of 1 week.
 - Daily incremental tape backups will be retained for at least 1 month.
 - Weekly full tape backups of logs will be retained for at least 1 month.
 - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to the Judicial Branch Help Desk. The Information Security Officer will be notified by Help Desk Personnel, ISO will then review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
 - Port-scan attacks
 - Evidence of unauthorized access to privileged accounts
 - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within Iowa Judicial Branch.
- Audits will be managed by Information Security Officer, in accordance with the *Audit Policy*. ISO will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal Iowa Judicial Branch Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History