ADMINISTRATIVE OFFICE OF THE COURTS
STATE OF NEW JERSEY

PHILIP S. CARCHMAN, J.A.D.
ACTING ADMINISTRATIVE DIRECTOR OF THE COURTS

RICHARD J. HUGHES JUSTICE COMPLEX
PO BOX 037
TRENTON, NEW JERSEY 08625

[Questions or comments may be directed to 609-292-0972.]

DIRECTIVE # 3-06

To: **ALL JUDICIARY COMPUTER SYSTEMS USERS**

From: **PHILIP S. CARCHMAN**

Subj: **JUDICIARY INFORMATION TECHNOLOGY SECURITY POLICY**

Date: **FEBRUARY 15, 2006**

PROMULGATION OF JUDICIARY IT SECURITY POLICY

This Directive promulgates the New Jersey Judiciary Information Technology Security Policy, as approved by the Supreme Court at its January 10, 2006 Administrative Conference. The Security Policy, which is effective immediately, supersedes the following previously approved directives and policies:

(1) Directive #6-98, Judiciary Policy on Access to Data Communications Networks (issued November 16, 1998);

(2) Directive #7-98, Judiciary Policy on Computer Software Copyright (issued November 16, 1998);

(3) Judiciary Internet Access and Use Policy as adopted by the Supreme Court on September 8, 1997;

(4) Electronic Mail Policy as approved by the Supreme Court on April 27, 2004.

DISTRIBUTION, ACKNOWLEDGMENT OF RECEIPT, AND INFORMATION SESSIONS

Every judge, staff person, contractor, and volunteer at the state, vicinage/county, or municipal level authorized to use Judiciary computer equipment will receive a copy of this Judiciary Information Technology Security Policy. Each such user will be required to sign a form acknowledging receipt of the policy. Each user also will be required to attend an informational session regarding the Security Policy. Supplementary memoranda setting out the details of these various implementation steps will be separately issued.

P.S.C.

Attachment
cc: Chief Justice Deborah T. Poritz

TABLE OF CONTENTS

INFORMATION TECHNOLOGY SECURITY POLICY

Introduction

The Judiciary relies on IT resources to handle large amounts of information that vary widely in type and in degree of sensitivity. This security policy is intended to establish standards for IT resource protection and to provide basic rules, guidelines, and definitions for all users. The goal is to prevent inconsistencies that can introduce risk, and create standards that serve as a fair and uniform basis for the enforcement of rules and procedures.

Effective security is a team effort involving the participation and support of all users. Your compliance with the security standards set forth in this policy is therefore crucial to safeguard the data the Judiciary holds, and crucial to maintaining the public's trust and confidence in the Judiciary.

Please carefully read the attached policy in its entirety. Some of the significant issues addressed in detail in the policy are:

- Passwords shall not be shared.
- Your workstation (PC) shall not be connected to any other network when it is connected to the Judiciary Network. If your workstation has a modem, the workstation must be disconnected from the Judiciary Network before you connect a phone line to the modem.
- Personal hardware and/or software shall not be installed on a Judiciary workstation or the Judiciary Network without prior authorization.
- All software installed on Judiciary workstations shall be licensed. Compliance with software copyright is required.
- A backup copy shall be kept of critical business data stored on your workstation.

- The integrity and confidentiality of electronic data shall be maintained during transmission, storage, and disposal.

- It is a violation of this policy to bypass, attempt to bypass, or assist another individual in attempting to bypass IT security measures established by the Judiciary.

INFORMATION TECHNOLOGY SECURITY POLICY

I. Purpose

The purpose of this policy is to establish a standard for safeguarding and securing the Judiciary's computers, computerized systems and data, computer networks, and technical infrastructure.

II. Scope

This policy applies to all persons authorized to access the Judiciary's computers, computerized systems, and computer networks, including but not limited to: judges, employees, municipal court employees; contractors; and volunteers. This policy shall be distributed to all such authorized persons (users). All such users shall acknowledge receipt of this policy and their responsibility for compliance by following the attached compliance procedure and acknowledgement form.

This policy does not apply to:

members of the public who anonymously use equipment provided and secured by the Judiciary for public use to access Judiciary public-access data;

members of the public who anonymously use the internet to access Judiciary public-access data; or

outside institutional users (e.g., Executive Branch employees, federal government employees) who are provided access to Judiciary computers by virtue of various cooperative agreements (a separate policy document will be promulgated in that regard);

III. No Personal Use/No Expectation of Privacy

Users are advised that computers, computer networks, E-mail and other electronic communications systems and all communications created, received, stored on or transmitted through these systems are Judiciary property. Accordingly, users shall not use these resources for personal use and have no reasonable expectation of privacy regarding this equipment, networks, systems, or these communications and are advised that the systems and their communications are subject to monitoring and interception by management. While the systems may contain passwords, locks, encryption or other security features provided to users, users are advised that these security features exist to protect the Judiciary's business interests and not to protect a user's personal use of a business resource.

IV. Routine Monitoring and Systems Maintenance

Authorized information technology personnel may access or monitor computer systems, networks, internet access/use, electronic mail, and other communications created, received, stored on or transmitted through these systems only in the course of system maintenance and repair, and only for purposes of assuring system performance and security or detecting breaches of that security. Any violation of this security policy discovered during such routine maintenance and monitoring shall be reported to the Administrative Director and the user's immediate supervisor.

V. Non-Routine Monitoring

Approval to access or monitor the computer systems, networks, internet access/use, electronic mail, and other communications of a user may be granted by the Administrative Director for any legitimate purpose, including but not limited to, the following circumstances:

- In the course of asserting a claim or legal defense of the State or a State employee in a civil action or administrative proceeding;
- Investigations of allegations of employee misconduct or violations of the law;
- Investigations of abuse of Judiciary resources;
- Investigations of breaches of security; and
- When a user is unavailable and the Judiciary must conduct business. Verification of a user's unavailability is required. In this instance, management should attempt to contact the individual and inform the individual prior to asking the Administrative Director for permission to access the individual's computer files.

VI. Information Sessions/Training

All authorized Judiciary users shall be informed or trained on this policy and its importance.

VII. Definitions

Access - To gain the ability to view, read, and/or copy the contents of a computer-generated and maintained file or records or the ability to connect to or use a network.

Disclosure - To expose a computer-generated and maintained file to someone other than the originator or to expose a user account (ID) and/or password to someone other than the assigned user.

Browser - A client program (software) that is used to access various kinds of Internet resources.

Client - A computer, or a software package, that is used to contact and obtain data from a Server software program on another computer.

Data Communications - Any technology such as telephone lines, radio transmission, etc. that carry computer-to-computer communications (as opposed to voice communications) such as court record data and electronic mail.

Electronic Mail - Non-interactive communication of text, data and images between a sender and designated recipients(s) by systems utilizing telecommunications links.

Intranet - A private network inside an organization that uses the same kinds of software that one would find on the public Internet, but that is only for internal use. An example is the Judiciary's Infonet.

LAN (Local Area Network) - A computer network limited to the immediate area, usually the same building or floor of a building with the purpose of interconnecting computers, printers, and servers.

Laptop - Portable PC – Full function portable computer assigned to mobile users. A laptop may have a modem or wireless communication capability.

PC - Personal Computer - A self contained computer that allows individuals to run a variety of commercial based and home applications.

PDA - Personal Digital Assistant – A PDA is usually a handheld device that can be used to organize and manage scheduling or notes. It can also integrate with other Office suites to share data or receive mail.

Modem (MOdulator, DEModulator) - A device that connects a computer to a telephone line, and allows the computer to communicate with other computers through the telephone system.

Monitor - The ability of a computer program or human to check, observe, test, track, or watch in order to detect errors, trends, discrepancies, opportunities, irregularities, and/or patterns.

Network - A connection of two or more computers that allows for the sharing of resources.

Password - A code used to gain access to a protected system.

Router - A special-purpose computer (or software package) that handles the connection between two or more networks or the connection between sites within a network.

Server - A computer, or a software package such as an email server, that provides a specific kind of service to client software running on other computers.

Spam - Unsolicited electronic mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, or individuals; junk e-mail.

Tablet - Portable PC – Small, lightweight, portable computer which allows handwritten and/or voice entry of data as well traditional data entry (keyboard, mouse). A tablet may have a modem or wireless communication capability.

Two-factor authentication - Authentication of a user accessing a network which requires the user to provide two pieces of identification. Such identification shall consist of 1) UserID/Password combination and 2) Additional key known only to the user. An example of item 2 may be a security hardware or software token combined with a unique PIN assigned by the user.

User Account (ID) – An ID or username assigned to an individual which is used to gain access to restricted data or other resources. User Accounts are used in conjunction with passwords which are usually established by the user.

WAN (Wide Area Network) - Any internet or network that covers an area larger than a single building or campus; A collection of LANs connected by data communication lines.

Workstation – A computer device assigned to an individual to use (PC, Notebook, Tablet, PDA (Palm, Blackberry, for ex.), etc.).

VIII. POLICIES

A. Data Security

1. The Judiciary shall ensure the integrity and confidentiality of data and the associated timely availability of systems to users.

2. Data shall be classified and protected based on, among other factors, its sensitivity and criticality to users, risks related to unauthorized disclosure, and legal and/or regulatory requirements.

3. Controls shall be established to ensure the data's validity, accuracy and completeness throughout all stages of data processing.

4. All Judicial systems which access restricted or protected data shall authenticate the identity of the user prior to allowing any access to the data.

5. All data shall be securely disposed of according to its sensitivity in an approved manner unless otherwise governed by legislative or regulatory requirements.

6. All critical business data stored electronically shall be backed up periodically to ensure its safety, for recovery of lost data, and for disaster recovery purposes.

7. No user shall intentionally alter, falsify, destroy, mutilate, backdate, or fail to make required entries on any electronic records or systems within the user's control.

8. Users shall not divulge any confidential data derived from any Judiciary information system.

B. Electronic Mail Security

1. Users should not treat the electronic mail system as a shared file system that is open to all users, and are prohibited from intercepting, monitoring or reading email messages that are sent, received, or stored in the email system by other users.

2. Users should be aware that documents created and sent by electronic mail for official business or as evidence of official acts may constitute official records of the Judiciary and/or the State. Any document created or sent by electronic mail, whether internally or externally through systems such as the Internet, is subject to this policy, and may be subject to other regulations, laws, or policies on public records.

3. The automatic forwarding of electronic mail from Judiciary email systems to personal email accounts is not permitted. Exceptions require authorization by the Assignment Judge or Trial Court Administrator in the Vicinages, or by the Administrative Director, Deputy Administrative Director, AOC Director, or Clerk of Court in the Central Office.

4. Use of copyrighted or trademarked logos in any electronic mail message text, or as part of a signature, is prohibited.

5. Use of union-related titles in Judiciary email systems electronic mail signatures is prohibited unless the email message is related to union business.

6. Use of Judiciary email systems for the distribution of chain letters and nuisance/spam messages is prohibited.

7. The use of the Judiciary email system for vulgar, abusive, offensive or inflammatory communication is not permitted.

8. Users who receive electronic mail containing confidential information shall take all necessary measures to ensure that confidentiality is maintained, and shall not disclose or transmit confidential information to any unauthorized persons.

C. Internet Security, Access, and Use

1. To control unnecessary Judiciary spending and avoid duplication of effort, separate access contracts with commercial Internet providers are not permitted without prior authorization by the Administrative Director.

2. User access to the Internet through established Judiciary facilities is offered as a tool for meeting the programmatic and operational needs of the Judiciary. Use of Judiciary-provided Internet access shall be in accordance with the relevant canons of the Code of Conduct governing Judiciary Employees, including but not limited to Canon 3.

3. Use of the Internet is a privilege which constitutes the acceptance of responsibilities and obligations that are subject to federal, state and local laws. Internet use shall be legal, ethical, and respectful of intellectual property, ownership of data, and systems security.

4. Requests for Internet access must be accompanied by a statement explaining the business need for such access.

5. Standards of Conduct for Use of Internet Services:

    a) The Internet is an unsecured system that has no security controls and shall never be used to transmit confidential or sensitive information, unless such transmissions are encrypted to ensure security. Encryption software used for such purposes shall conform to established standards.

    b) Users shall not act as spokespersons by attempting to answer every survey/question asked by the public via the Internet, unless authorized to do so. Users shall reply only to those questions that are within the scope of their work for the Judiciary. Users shall handle Internet inquiries about Judiciary matters that are outside the immediate scope of work as they would handle similar telephone inquiries.

    c) Users shall not give out personal information (such as home address, home telephone number, credit information, etc.) about themselves or other users when responding to any member of the public on behalf of the Judiciary

    d) The privilege of Judiciary provided access to the Internet may be revoked at any time for inappropriate conduct.

Examples of inappropriate conduct include (but are not limited to):

i. use of the Internet that violates the Code of Conduct for Judiciary Employees;

ii. use of the Internet for unlawful activities;

iii. use of abusive or objectionable language in either public or private messages;

iv. misrepresentation of oneself or the Judiciary;

v. activities that could cause congestion and disruption of networks and systems; and

vi. activities that could cause security risks or problems which are not addressed by existing controls.

D. Local Area Network Security

1. The New Jersey Judiciary has implemented local area networks which provide data communications within individual Judiciary sites state-wide. These networks have been established to facilitate the performance of Judicial Branch functions and are intended for official business only.

2. Requests for local area network access shall identify the business need for such access.

3. Access to local area networks shall comply with approved security measures. No user shall bypass or assist another person in bypassing established security measures.

4. No user may connect any hardware or software not provided by the Judiciary to a Judiciary local area network without prior written approval by ITO or the local IT Manager. Any such approval is contingent upon compliance with established security measures.

5. Local area networks are established by the AOC/ITO and the local IT support staff using dedicated data communications facilities connected to specialized data communications equipment (Server, Switch, Hub, Wireless Access Point, etc.). Only ITO and the local IT staff are permitted to install, configure, and maintain local area network facilities and equipment.

6. Local area networks are connected to the Judiciary wide-area network by the AOC/ITO using specialized communications equipment (such as routers). Only ITO staff are permitted to install, configure and maintain such equipment and connections.

7. Access to shared server resources (such as applications, file storage, printers) on a Judiciary local area network is provided to users by the local IT staff or AOC/ITO using established security measures. No user may attempt to bypass established security measures to gain access to shared server resources which have not been authorized.

8. Wireless Access Points are prohibited on a Judiciary local area network unless approved by the AOC/ITO and must use established security measures. This includes the setup and verification of the devices to ensure that current wireless access standards are applied. No user may attempt to bypass established security measures.

9. No computer equipment may be simultaneously connected to both a Judiciary local area network and any wide-area network beyond the Judiciary WAN, through a modem, wireless modem, or equivalent device.

10. No user connected to a Judiciary local area network may use either a hardware device or software (such as PCAnywhere, Reachout, Carbon Copy, Languard, VNC) to access, capture, or control another Judiciary PC unless authorized to do so by ITO or the local IT Manager. Access will only be provided through established Judiciary security systems.

E. Password Security

1. General Requirements: Passwords are an important aspect of computer security and are usually the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Judiciary's entire enterprise network. As such, all users are responsible for taking the appropriate steps, as outlined below, to secure their passwords.

    a) All system-level passwords (e.g., root, enable, server admin, application administration accounts) must be changed at least every ninety days, and must be unique from user-level passwords.

    b) All user-level passwords (e.g., e-mail, applications, Web, desktop computer) must be changed at least every ninety days.

    c) Passwords must not be inserted into e-mail messages or other forms of electronic communication.

2. Passwords should never be written down (unless stored in a locked safe for recovery purposes) or stored online.

3. Passwords shall not be shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Judiciary information.

4. Application developers must ensure their systems comply with established security measures.

F. Office Security

1. Users hosting visitors in secure areas within Judiciary offices which contain IT equipment are responsible for ensuring that such visitors comply with established security measures. Should any visitor fail to comply with established security measures, they shall be reported to the appropriate security officials.

2. Users are responsible for controlling access to Judiciary computer equipment issued to them and must take reasonable care to ensure that such equipment is not accessed by unauthorized persons.

3. Only AOC/ITO, local IT staff, or other authorized individuals may relocate Judiciary computer equipment. Other authorized individuals may only relocate equipment specified on a Judiciary Property Removal Authorization. IT staff who contract for a third party to relocate equipment must ensure that the third party handles the computer equipment in a secure manner.

4. Users removing Judiciary computer equipment from a Judiciary office must comply with established property removal procedures.

5. Obsolete computer equipment must be disposed following the Judiciary's surplus property procedures.

6. Computer equipment and networks installed in Judiciary offices are the property of the Judiciary and may be installed, configured, modified, or accessed only by authorized personnel. This includes personal computers and printers, network servers, local area network wiring, hubs, switches, routers, modems, DSU/CSUs, wireless access points, UPSs, and similar equipment and facilities including telephone closets and computer rooms.

G. Wide Area Network Security

1. The New Jersey Judiciary has implemented a wide-area network which provides data communications among locations state-wide including the Judiciary, the New Jersey Executive Branch and related governmental agencies (County Jails, Municipal Parking Authorities, County Prosecutors, Public Defenders), and the Internet. This network has been established to facilitate the performance of Judicial Branch functions and is intended for official business only.

2. Requests for access to the Judiciary wide area network shall identify the business need for access. All such access shall be through approved security measures. No user shall assist another person in bypassing established security measures.

3. Site-to-site wide-area network access is established by the AOC/ITO using dedicated data communications facilities connected to specialized data communications equipment (router, modem). Only AOC/ITO staff are permitted to install, configure, and maintain site-to-site data communications facilities and equipment.

4. Dial access to the Judiciary wide-area network may be provided to users using Judiciary assigned equipment (PC, Laptop, Tablet, PDA). Such equipment is configured by Judiciary IT staff to comply with established security measures. Users shall not alter the established security configuration of such equipment. Dial access to the Judiciary wide-area network requires two-factor authentication of the user.

5. Access to the Judiciary wide-area network through a personal connection to the Internet may be provided to users. Access may be provided from either Judiciary assigned equipment or the user's personal equipment at the discretion of AOC/ITO. Judiciary assigned equipment is configured by Judiciary IT staff to comply with established security measures. Users shall not alter the established security configuration of such equipment. Access through the user's personal equipment shall be limited to Internet browser access to specific applications such as email and shall use ITO established security measures which will not alter the configuration of the user's personal equipment. In either case, access requires two-factor authentication of the user.

6. No user connected to the Judiciary wide-area network may use either a hardware device or software such as PCAnywhere, Reachout, Carbon Copy, Languard, or VNC to access, capture, or control another Judiciary PC unless authorized to do so in writing by ITO or the local IT Manager and unless access is through approved AOC/ITO security systems.

H. Workstation Security

1. The New Jersey Judiciary has provided personal computing equipment (workstations) and licensed software to users. This equipment and software have been established to facilitate the performance of Judicial Branch functions and are intended for official business only.

2. Judiciary provided workstations may be connected to a Judiciary local area network (LAN) only by the AOC/ITO or local IT support staff. Where security circumstances dictate and Judiciary business needs can still be fulfilled as determined by ITO or the local IT Manager, certain workstations shall not be connected to a Judiciary LAN.

3. The Judiciary has established security measures relating to the configuration and use of LAN-attached workstations. No user may bypass these established security measures.

4. The Judiciary has provided workstations for the public to access Judiciary records. These workstations may be connected to a Judiciary LAN depending on the need to access LAN or mainframe based data. The Judiciary has established security measures relating to the configuration and use of Public Access workstations. No user may bypass these established security measures.

5. Wireless access to a Judiciary LAN or WAN is prohibited without written approval. Such access must use established security measures. This includes the setup and verification of the wireless devices (modem or LAN card) to ensure that current wireless access standards are applied. No user may attempt to bypass established wireless security measures.

6. No workstation may be simultaneously connected to both a Judiciary local area network and any wide-area network beyond the Judiciary WAN through a modem, wireless modem, or equivalent device.

7. No user may connect any personal hardware to or install personal software on a Judiciary workstation without written approval by ITO or the local IT Manager. Any such approval is contingent upon compliance with established security measures.

8. External media (diskette, CD, CD/ROM, DVD, tape, PCMCIA card, USB memory, etc.) shall be verified to be free of any software deemed to be a security threat prior to being used in a Judiciary workstation.

9. Users shall treat data stored on a Judiciary workstation as cautiously as they would use any non-digital communication medium, such as a letter or memorandum.

10. Any proprietary software in use on individual judiciary workstations and judiciary local area networks shall have a legal software license. Most software is licensed for use on one workstation only, and by one user at a time (except LAN versions). Software can be transferred to another workstation only if all copies of printed and machine readable (software) materials are transferred. Some special purpose and public domain software are not subject to license agreements. Users are responsible for reading and complying with each software license agreement.

IX. Compliance and Violations

After reviewing this policy statement, Users shall complete the attached Acknowledgement Form and return it to the appropriate Human Resources office as identified on the form.

Use of the Judiciary's computerized systems and networks is a privilege that may be revoked at any time, without notice. It is subject to existing policies including, but not limited to the Rules of Court, the Code of Conduct for Judiciary Employees, and the Judiciary's Equal Employment Opportunity, Affirmative Action and Anti-Discrimination Policy.

Access to the Judiciary's computerized systems and networks may be revoked based on violations of this policy and any standards and guidelines referenced herein.

Additionally, users violating this policy may be subject to disciplinary action, including but not limited to termination of employment, revocation of contracts and agreements, denial of service, and criminal and civil penalties.

S A M P L E

NEW JERSEY JUDICIARY

ACKNOWLEDGMENT OF RECEIPT FORM FOR THE JUDICIARY INFORMATION TECHNOLOGY SECURITY POLICY

I understand that, as a person (user) authorized to access the computers, computerized systems, and computer networks of the New Jersey Judiciary, I am subject to the New Jersey Judiciary Information Technology Security Policy as adopted by the New Jersey Supreme Court. I hereby acknowledge receipt of a copy of New Jersey Judiciary Information Technology Security Policy and agree to abide by its provisions.

NAME (printed) _____

SIGNATURE_____ DATE_____

CATEGORY OF SYSTEMS USER
(check one and complete further information as appropriate)

_____ Employee (Title:_____)

_____ Contractor

_____ Volunteer

_____ Other (Explain:_____)

COURT OR OFFICE _____

DIVISION OR UNIT _____

S A M P L E

NEW JERSEY JUDICIARY

JUDGE'S ACKNOWLEDGMENT OF RECEIPT FORM FOR THE JUDICIARY INFORMATION TECHNOLOGY SECURITY POLICY

I understand that, as a judge (user) authorized to access the computers, computerized systems, and computer networks of the New Jersey Judiciary, I am subject to the New Jersey Judiciary Information Technology Security Policy as adopted by the New Jersey Supreme Court. I hereby acknowledge receipt of a copy of New Jersey Judiciary Information Technology Security Policy and agree to abide by its provisions.

NAME (printed) _____

SIGNATURE_____ DATE_____

TITLE_____

COURT_____