STATE OF MARYLAND
JUDICIARY

POLICY ON ELECTRONIC COMMUNICATIONS SYSTEMS USAGE

I. PURPOSE

The purpose of this issuance is to establish a policy for the use of the Judiciary's electronic communications systems, including the hardware, software, electronic messaging (e-mail), Internet, and Intranet (collectively, "JIS system(s)"). These systems are provided to facilitate official business of the Judiciary of Maryland. This policy is to guard against uses, which are illegal or detrimental to the official business of the Judiciary or adversely affect the user's performance of their duties for the Judiciary while providing for limited, appropriate personal use.

II. DEFINITIONS

A. Administrative Official – The Clerk of Court in which an employee works; the Administrative Clerk or Administrative Commissioner of the District Court for the district in which an employee works; ~~or~~ the director of the respective department or office within the Courts of Appeal, the District Court Headquarters, or the Court-Related Agency in which an employee works; or the State Court Administrator for employees within the Administrative Office of the Courts.

B. Employee – Any person employed by the Judiciary (whether regular, contractual, temporary or a volunteer), except a judge or the elected Clerk of the Court.

C. User – Any person authorized to access the JIS systems, including, but not limited to, judges, the elected clerks of the court, employees and contractors.

D. Personally Identifiable Information – Any piece of information that potentially can be used to uniquely identify, contact or locate an individual.

III. SCOPE

This policy applies to all users of JIS systems. Courts not using JIS-provided systems for their electronic messaging (e-mail), Internet, Intranet, and online applications are required to have a substantially similar written policy on electronic communications systems usage.

IV. POLICY STATEMENT

Electronic communications systems, including the Internet, Intranet, e-mail and online applications are intended to increase user productivity in the conduct of their official

duties with the Judiciary. Inappropriate use of information systems or electronic communications, as defined below, is prohibited. Users are advised that electronic communications are not subject to personal privacy and may be disclosed pursuant to public disclosure laws and rules of discovery in the event of lawsuits.

V. RESPONSIBILITIES OF USERS

A. Permitted Use

1. Each user of JIS systems must exercise individual responsibility and judgment to assure the appropriate use. These systems are designed to afford electronic communications for official judicial business. In using email, users must ensure that all messages are courteous, professional and business-like.

2. Incidental personal use is permissible so long as: (a) it does not consume more than a minimal amount of resources; (b) does not interfere with user productivity; and (c) does not preempt any work-related activity.

   Users should not use a non-JIS system e-mail account (such as comcast.net, yahoo.com, gmail, or a similar account) for sending and receiving personal email. In the event that JIS posts a list of approved secure private e-mail account providers, users may not use a provider that is not on the list.

   Personal messages sent by employees using a JIS system e-mail account must be identified as “personal” in the subject designation, to avoid any confusion with official judicial business.

3. Users should always use care in addressing e-mail messages to make sure that messages inadvertently are not sent to unauthorized persons. When using distribution lists, users should confirm that all addresses are appropriate recipients of the information to avoid distribution to unintended or unauthorized recipients.

4. Users should use the “Reply to All” feature only when necessary for official purposes and after carefully reviewing the list of included addressees. Any user involved in an e-mail dialogue that generates multiple messages, should delete previous messages that are not necessary to the next addressees. Users are advised to save valuable disk space on the server and/or personal computer by deleting unnecessary messages.

B. Unauthorized Use

1. Users will not use JIS systems for commercial gain, or for any gaming or gambling purpose. Users will not use these systems to harass, intimidate or otherwise annoy another person. Users will not disclose personal

information about another person without that person's permission or other authorization.

2. Users will not use JIS systems for unlawful, unethical or unprofessional purposes or to support or assist such purposes.

   Examples of these impermissible uses may include, but are not limited to, the transmission or interception of violent, threatening, defrauding, obscene or otherwise illegal or unlawful materials, and the use of JIS systems for purposes related to any public election.

   Users will not use JIS systems, or any part of JIS systems, for any purpose that

   a. Adversely affects the primary purpose of the JIS systems;
   b. Causes harm to the JIS systems or any of its components;
   c. Is illegal or detrimental to the official business of the Judiciary;
   d. Adversely affects the user's performance of his or her duties for the Judiciary; or
   e. Is for any political purpose.

3. Users shall be vigilant in guarding against the improper or malicious disclosure of confidential or personally identifiable information.

4. Users will not use JIS systems to disrupt other users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses, and sustained high volume network traffic, which substantially hinders others in their use of JIS systems.

5. Confidential information should never be transmitted or forwarded to individuals or companies not authorized to receive that information. Confidential information may be sent or forwarded to other Maryland Judiciary users only as necessary for official purposes.

   An employee may not subscribe to services provided by a List Server, which automatically redistributes e-mail to names on a mailing list, unless related to official or professional purposes.

6. Employees, except Judges or Administrative Officials, may not send file attachments through e-mail unless those file attachments are for official purposes.

7. Users may not copy and/or transmit any files, software, or other information that in any way violates any Federal or state copyright law.

8. Users may not use JIS systems inconsistent with: any law; the Maryland Code of Judicial Conduct; personnel rules, policies or regulations; or accepted community standards.

VI. RESPONSIBILITIES OF JIS SYSTEM ADMINISTRATION

A. User Access and Training

1. JIS will provide access to JIS systems for all authorized users as directed by the Chief Judge of the Court of Appeals.

2. JIS will provide training to authorized users in the proper use of JIS systems, when requested to do so.

B. Monitoring

1. The right to use JIS systems does not include the right to privacy.

2. JIS may monitor access and use of JIS systems for network management and security purposes.

3. JIS will notify the appropriate Administrative Official when JIS finds evidence of use of JIS Systems inconsistent with this Policy.

4. Nothing in this Policy is intended to limit the right of an Administrative Official or Chief Judge to monitor a user's use of JIS Systems to investigate any complaint or an Administrative Official's concern that use of JIS Systems is inconsistent with this Policy.

C. System Security

1. All acquisitions of information systems components will be coordinated through JIS. This includes demonstration hardware and software used for evaluation purposes as well as products acquired for ongoing use.

2. All users are responsible for caring for the personal computer system components that they are assigned or used. Users are responsible for promptly reporting any equipment, software and data damage and/or destruction of which they become aware.

3. The JIS computer system is designed to work in a network environment. Installation of unauthorized software can result in damaging the integrity of the system. Employees are responsible for obtaining the approval of their Administrative Official and JIS before downloading or installing software on any JIS-issued computer.

4. Users are prohibited from using loopholes or knowledge of a special

password to damage computer systems, obtain extra resources or to gain access to systems for which proper authorization has not been given.

5. No Administrative Official or supervisor may authorize the use of unlicensed or copied software on any JIS-issued computer.

VII. FAILURE TO COMPLY

A. Failure by a user to comply with the provisions of this policy may lead to remedial action.

B. Remedial action may include revocation or other limitation of access to electronic communications; disciplinary proceedings against the individual or individuals responsible for the violation of this policy, including termination of employment; or referral to the appropriate disciplinary authority.

C. Violation of this policy by a user is subject to remedial action pursuant to the supervisory authority of the user's Administrative Official.

VIII. INTERPRETIVE AUTHORITY

A. Subject to paragraph B, the Judiciary Human Resources Department, in consultation with other parties, as appropriate, is responsible for the interpretation of this policy.

B. The Chief Judge of the Court of Appeals; the Chief Judge of the Court of Special Appeals; the Chief Judge of the District Court; the respective administrative judges; and the respective elected clerks of the court shall be responsible for the implementation and interpretation of this policy as to users for whom they have ultimate supervisory or administrative responsibility.