ADMINISTRATIVE DIRECTIVE NO. 159

This 22nd day of September, 2006

IT APPEARS THAT:

(1) It is necessary to ensure the security of the computer network and the integrity of data stored on State systems.
(2) It is important that use of communications and computer systems conforms to applicable laws and appropriate standards so that these systems are not used in ways that could be disruptive to the network, result in liability, or incur unnecessary expense.
(3) All employees using communications and computer systems should have written notice of what constitutes acceptable and unacceptable use, including those circumstances under which personal use is acceptable.
(4) To achieve these objectives, while ensuring that necessary confidentiality is maintained, it is desirable to adopt a Judicial Branch Authorized Use Policy for the Communications and Computer Systems.

NOW THEREFORE, IT IS DIRECTED, with the unanimous approval of the members of the Supreme Court, pursuant to Del. Const. Art. IV, § 13(1), that:

(1) The Judicial Branch Authorized Use Policy for the Communications and Computer Systems ("Policy"), attached hereto, is hereby adopted.

(2) Each court and agency within the Judicial Branch are directed to implement this Policy with regard to both existing and new employees within 30 calendar days from the date of this Administrative Directive.

(3) The State of Delaware's Department of Technology and Information concurs with the provisions of this Policy, and the signed concurrence of Secretary Thomas M. Jarrett, Chief Information Officer, has been obtained and is on file in the State Court Administrator's office.

BY THE COURT:

Chief Justice Myron T. Steele

JUDICIAL BRANCH
AUTHORIZED USE POLICY FOR THE COMMUNICATIONS AND COMPUTER SYSTEMS

POLICY

This policy adopts, with specified changes, the provisions of the **Department of Technology & Information Acceptable Use Policy** as the **Authorized Use Policy for the Communications and Computer Systems for Judicial Branch Personnel.** A copy of the DTI policy is attached to this policy, and can also be found on the internet at: http://dti.delaware.gov/information/AUP.pdf .

ACKNOWLEDGEMENT OF COMPLIANCE

Judicial Branch personnel will receive a copy of this policy through e-mail, and/or in writing, as a part of employee orientation, and upon implementation of this, and subsequent, versions of this policy. All Judicial Branch personnel (including judicial officers) are required to sign a form acknowledging that they have read and agree to abide by this policy. The form may be either a separate form pertaining to the Authorized Use Policy specifically, or contained within a general acknowledgment form covering all policies of the Court and/or the Judicial Branch and specifically mentioning the Authorized Use Policy. Forms shall be maintained in the personnel files of each court or agency.

ENFORCEMENT

Any improper use of State communications and computer systems may be grounds for disciplinary action or other sanction, as appropriate to the offense and pursuant to applicable codes or rules.

MONITORING

State communications and computer systems, including, but not limited to, computer networks, data files, e-mail and voice mails, may be monitored and/or accessed by the State to ensure the integrity of the network, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes. In order to safeguard the integrity of shared network resources and protect computer systems against security threats, procedures may be implemented for monitoring network traffic, logging errors and exceptions and performing industry-standard maintenance. JIC and DTI will neither conduct any content-based monitoring nor permit any other party to conduct content-based monitoring of usage by Judicial

Branch personnel, except upon prior notice to and the written approval of the Chief Justice of the State of Delaware, unless maintaining the security or integrity of the network requires immediate action. In that situation, the Chief Justice will be notified, and his approval sought, as soon as possible in the process.

DELAWARE JUDICIAL BRANCH
AUTHORIZED USE POLICY AGREEMENT FORM

This is to certify that I have read and agree to abide by the guidelines set forth in the Judicial Branch Authorized Use Policy for Communications and Computer Systems.

Name: _____

Signature: _____

Court/Judicial Branch Agency: _____

Date: _____

Delaware DEPARTMENT OF TECHNOLOGY & INFORMATION *Enabling Excellence In Delaware State Government*	STATE OF DELAWARE **DEPARTMENT OF TECHNOLOGY AND INFORMATION** 801 Silver Lake Blvd. Dover, Delaware 19904

Doc Ref Number:	DTI-0042.02	**Revision Number:**	3
Document Type:	External Policy	**Page:**	1 of 11
Policy Title:	Acceptable Use Policy		

Synopsis:	Guide Behaviors in Using the State's Communications and Computer Systems		
Authority:	Title 29, Delaware Code, §9004C – General powers, duties and functions of DTI "2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transportation facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State's informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;		
Applicability:	All users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.		
Effective Date:	June 5, 2006	**Expiration Date:**	None
POC for Changes:	DTI Chief Security Officer		
Approval By:	Cabinet Secretary - State Chief Information Officer		
Approved On:	June 5, 2006		

TABLE OF CONTENTS

Section		Page
I.	**Policy**	2
II.	**Definitions**	9
III.	**Development and Revision History**	9
IV.	**Approval Signature Block**	9
V.	**Listing of Appendices**	9

I. Policy

A Message to all System Users

This document formalizes the State policy for state agency and public school district employees as well as contractors and other "users" of our State's communications and computer systems. Each agency/school district or affiliate may also choose to develop and enforce its own acceptable use policies to further restrict the use within its local environment. This may be done only with the understanding that, should a conflict exist, the State's Acceptable Use Policy (AUP) takes precedence over all local policies developed within the agencies/affiliates for the explicit purpose of exercising responsible controls at the local level.

Our goal is to put controls in place that will help protect the State from sabotage and espionage. The threat is real, as each month, DTI intercepts tens of thousands of viruses and suspicious messages containing executable files trying to bypass our security systems. These controls also help minimize the potential risks of misuse. This misuse includes unnecessary Internet usage causing network and server congestion. This Acceptable Use Policy is your (the user's) guide for helping us achieve this goal by conducting State of Delaware business with integrity, respect, and prudent judgment. Each of us is responsible for upholding the State's commitment to the highest standards of conduct.

> **Affiliates include the Judicial Branch, the Legislative Branch, and other State & Local government political subdivisions authorized to use these state services.*

Users are accountable for familiarizing themselves with this policy and using it as a guidepost for your daily decisions and actions when using these services.

Each agency/school district and affiliate organization(s) are responsible for the activity of its

users and for ensuring that its users follow this Acceptable Use Policy. Violations, which are not promptly remedied by the client organization, may result in termination of these services.

Introduction

This Acceptable Use Policy is your resource to help you make sound decisions in using communications and computer systems to do your job.

All of us have a responsibility to:

Read: the policy and give careful attention to those subjects that most pertain to your job duties.

Understand: the purpose of this policy and your overall responsibilities for standards of business conduct.

Consult: your supervisor or organization's Information Resource Manager (IRM) for additional clarification of this policy.

Note the Following:

Applicability

State of Delaware's expectations for responsible use are applicable to all parties who use the State communications and computer systems on behalf of the State, including, but not limited to, its agency, school district, and affiliate employees, consultants, in-house contractors, and other "users."

Limitations

This acceptable use policy does not address every expectation or condition regarding acceptable use. It does not substitute for other more specific State policies and procedures.

Acknowledgement Statement

As part of this policy, each network user is required to read and understand the AUP and sign the acknowledgement statement in Appendix 1. There is a version for state employees as well as non-state employees. We encourage organizations to have their staff review the AUP annually. The signed acknowledgement statement must be maintained by your organization in the personnel file. Network users who do not sign the Acceptable Use Policy Acknowledgement Statement will be denied access to the State's Communications and Computer Systems.

Acceptable Use of Communications and Computer Systems

State of Delaware communications and computer systems are vital to our business and critical to overall communications. Our success is directly related to safeguarding and properly using these systems.

WHAT ARE STATE COMMUNICATIONS AND COMPUTER SYSTEMS?

State of Delaware communications and computer systems are any equipment, hardware,

software or networks (including wireless networks) owned, provided or used by or on behalf of State of Delaware that store or transmit voice or non-voice data. This includes telephones, cellular/wireless telephones, voice mail, computers, e-mail, facsimiles, pagers, and State Intranet or Internet access (including when accessed through personal computers).
Note: When personal computers are not owned by the state but are used for State business, the State retains the right to access any State records or materials developed for State use. Also, we must ensure that any State materials are appropriately safeguarded according to applicable standards in this section, including, but not limited to, virus protection of, protected access to and backup of these materials

Access, Maintenance and Protection

Users must safeguard the confidentiality and integrity of State systems, including strong password logons (see Strong Password Standard), access codes, network access information, log-on IDs) from improper access, alteration, destruction and disclosure. Users shall only access or use these systems when authorized. Users must abide by State standards contained in this section and other State policies regarding protecting data and information stored on these systems. State standards are available at http://dti.delaware.gov/information/standards-policies.shtml.

Unlawful and Inappropriate Use

Users are obligated to never use State systems (such as the Intranet or Internet) to engage in activities that are unlawful, violate State policies or in ways that would:

- Be disruptive, cause offense to others, or harm morale.
- Be considered harassing or discriminatory or create a hostile work environment.
- Result in State of Delaware's liability, embarrassment or loss of reputation.

External groups or organizations are not permitted to make announcements, solicitations or otherwise access the State's Communications and Computer Systems, except as permitted by law.

Protection and Integrity of Data

Users must maintain the integrity of State Information and data stored on State systems by:

- Only introducing data into our systems that serves a legitimate business purpose.
- Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
- Protecting data and information stored on or communicated across our systems and not accessing this data or information (for example, agency data, employee records) unless authorized.
- Protecting data and information communicated over internal or public networks (for example, the Internet) to avoid compromising or disclosing nonpublic State Information or communications. Organizations and employees are required to perform a FOIA analysis to determine whether information is disclosable or protected under the statute, and should seek legal counsel for an opinion when in doubt. The protection of data and information applies to all electronic venues that the State might be using such as email, web applications, social media, etc.
- Protect data and information by not auto-forwarding State email to non-authorized individuals.

Personal Use

While State systems are intended for primarily business/instructional purposes, limited (incidental and occasional) personal use may be permissible when authorized by your management and it does not:

- Interfere with your work responsibilities or business/instructional operations.
- Involve interests in personal outside business and/or other non-authorized organizations and activities (which may include, but is not limited to selling personal property/items or soliciting for or promoting commercial ventures, charitable, religious or political activities or causes).
- Violate any of the standards contained in this code or other State of Delaware policies.
- Lead to inappropriate costs to the State. (Excessive personal surfing, utilizing streaming services for personal use such as listening to music or watching video, and downloading of music and video files are *specifically forbidden*.)

Virus Protection

Users must check all electronic media, such as software, diskettes, CD-ROMs and files for viruses when acquired through public networks (for example, the Internet) or from outside parties using virus detection programs prior to installation or use. If users suspect a virus, they must not use the applicable computer systems and equipment until the virus is removed and they will report the matter immediately to the appropriate network security contact. The Department of Technology and Information has purchased anti-virus software for all government sites including home computers. Similarly the Delaware Center for

Educational Technology has purchased anti-virus software for all public K-12 schools.

Properly Licensed Software
Users will only use approved and properly licensed software and will use it according to the applicable software owner's license agreements.

Treatment of Third-Party Data or Software
Users must ensure that any nonpublic State Information or software of a third party that is stored, copied, or otherwise used on State systems is treated according to State of Delaware's standards regarding nonpublic State Information and applicable agreements and intellectual property restrictions.

State of Delaware Monitoring
State communications and computer systems, including, but not limited to, computer networks, data files, e-mail and voice mail, may be monitored and/or accessed by the State to ensure the integrity of the technology, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes. Although the Department of Technology and Information (DTI) does not randomly monitor message or network transactions, DTI may without notification or approval, monitor, access and review any and all communications originating from the State of Delaware or delivered to the State of Delaware – employees should have no expectation of privacy in regard to use of these services. This is in accordance with 19 Del. C. chapter 7.

USE OF EMAIL AND THE INTERNET

Inappropriate use of e-mail includes, but is not limited to, sending or forwarding:

- **Messages, including jokes or any language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive or otherwise inappropriate (this includes but is not limited to, messages about age, race, gender, disability, sexual orientation, national origin or similar matters).**
- **Pornographic or sexually explicit materials.**
- **Chain letters.**
- **Information related to religious materials, activities or causes, including inspirational messages.**
- **Charitable solicitations unless sanctioned by State of Delaware.**
- **Gambling.**
- **Auction-related information or materials unless sanctioned by State of Delaware.**
- **Games or other software or copyrighted materials without a legitimate business or instructional purpose (and then only according to the rights and**

licenses granted by the owner of the games, software or copyrighted material).

- **Messages that disparage other companies or products.**
- **Large personal files containing graphics materials or audio files (such as photographs and music).**
- **Materials related to personal commercial ventures or solicitations for personal gain (for example, messages that could be considered pyramid schemes).**
- **Information related to political materials, activities or causes unless sanctioned or permitted by the State of Delaware.**
- **Unauthorized or inappropriate mass distribution of communication.**
- **Any other materials that would be improper under this policy or other State of Delaware policies.**

Inappropriate use of the Internet includes, but is not limited to, accessing, sending or forwarding information about, or downloading (from):

- **Sexually explicit, harassing or pornographic sites.**
- **"Hate sites" or sites that can be considered offensive or insensitive.**
- **Auction or gambling sites.**
- **Non State of Delaware business-related chat sites.**
- **Underground or other security sites which contain malicious software and/or instructions for compromising State of Delaware security.**
- **Games, software, audio, video or other materials that we are not licensed or legally permitted to use or transmit or that are inappropriate, or not required by, State of Delaware business or instruction.**
- **Offensive or insensitive materials, such as sexually or racially oriented topics.**
- **Any other materials that would be improper under this policy or other State of Delaware policies.**

Inappropriate use of the Internet also includes:

- **Intentional importation of viruses.**
- **Registering Internet domain names of the State of Delaware business/school district or those of third parties without authorization from DTI.**

Note: In order to perform their job duties (for example, network monitoring), specific State of Delaware employees may receive management approval exempting them from some of the above restrictions.

REMEDIAL ACTION

Network users who do not sign the Acceptable Use Policy Acknowledgement Statement in Appendix 1 will be denied access to the State's Communications and Computer Systems.

When DTI learns of a possible inappropriate use, DTI will immediately notify the agency/school district or affiliate responsible, which must take immediate remedial action

and inform DTI of its action. In instances where agencies/school districts or affiliates do not respond in a timely or reasonably appropriate manner, are "repeat offenders", or if criminal activity is suspected, DTI will work directly with the proper authorities, and follow their guidance in determining appropriate action.

Any inappropriate use of State communications and computer systems may be grounds for discipline up to and including dismissal based on the just cause standard set forth by Merit Rules, or collective bargaining agreement, whichever is applicable to the subject employee. Exempt employees shall be subject to appropriate discipline without recourse, except as provided by law.

In an emergency, in order to prevent further possible unauthorized activity, DTI may temporarily disconnect that agency or affiliate. If this is deemed necessary by DTI staff, every effort will be made to inform the agency or affiliate prior to disconnection, and every effort will be made to reestablish the connection as soon as it is mutually agreed upon.

Any determination of non-acceptable usage serious enough to require disconnection will be promptly communicated to the Senior Manager at the agency or affiliate by the DTI Executive Team.

Unauthorized activity or non-acceptable usage determined at the agency/school district or affiliate may be subject to remedial action being taken in accordance with the acceptable use policy of that agency/school district or affiliate as well as those actions outlined above. The remedial action outlined in agency/school district or affiliate policies may differ from the remedial action as outlined in this policy.

DTI provides access to state, national and international resources to its clients through connections with networks outside of Delaware. In general, it is the responsibility of those networks to enforce their own acceptable use policies. DTI will make every attempt to inform its clients of any restrictions on use of networks to which it is directly connected; as such information is made available by the network provider.

DTI accepts no responsibility for traffic that violates the acceptable use policy of any directly or indirectly connected networks beyond informing the client that they are in violation if the connected network so informs DTI.

RELATED POLICIES:

This policy must be used in concert with other policies and standards in order to be effective. Those that are especially applicable are listed below:

State of Delaware Information Security Policy

Strong Password Standard

QUESTIONS OR COMMENTS ON THIS POLICY

1. Users should offer comments or seek clarification through their supervisor or Agency/School District or Affiliate IRM.
2. Agency/School District or Affiliate IRM's should offer comments or seek clarification by sending an email to eSecurity@state.de.us

II. Definitions

None

III. Development and Revision History

Initial version established April 15, 2003.
Corrected hyperlinks, reference to the Merit rules, and CRS title change on August 8, 2005.
First reformatted version established July 31, 2006.
Revised version published on May 22, 2007.
Updated acknowledgement statement on September 17, 2007.
Clarified the requirement to sign the Acknowledgement statement in Appendix 1 on September 5, 2008.
Add FOIA and social media topics on July 1, 2009.

IV. Approval Signature Block

On File	
Name & Title: Cabinet Secretary - State Chief Information Officer	**Date** June 5, 2006

V. Listing of Appendices

Appendix 1 – Acknowledgement Statement

Delaware
DEPARTMENT OF TECHNOLOGY & INFORMATION
Enabling Excellence In Delaware State Government

ACKNOWLEDGMENT STATEMENT

State Of Delaware - Acceptable Use Policy

State Employee

This is to certify that I have read and agree to abide by the guidelines set forth within the State Acceptable Use Policy. As an employee of the State of Delaware, I fully intend to comply with this policy realizing that I am personally liable for intentional misuse or abuse of the State's communications and computer systems. If I have any questions about the policy, I understand that I need to ask my supervisor or IRM for clarification. Users are also encouraged to take and score 100% on the AUP self-test located on the DTI Internet at: http://dti.delaware.gov/information/aup_self_test.shtml

If I refuse to sign this acknowledgement form, my supervisor will be asked to sign to this form indicating that I have been given time to read and have questions answered about this policy. The supervisor will read this statement to me prior to signing the document and advise me that by not signing this document my rights to use the State's Communications and Computer Systems will be denied and may affect my ability to meet my job requirements.

Name: _____

Signature: _____

Agency/Organization/School: _____

Date: _____

****

Supervisor Signature
(*as required): _____

Comments: _____

_____

Delaware
DEPARTMENT OF TECHNOLOGY & INFORMATION
Enabling Excellence In Delaware State Government

Non-State Employee (All Other Users)

This is to certify that I have read and agree to abide by the guidelines set forth within the State Acceptable Use Policy that apply to my use. (Some users may use a combination of communications and computing resources) As an authorized user of the State of Delaware's communications and computing resources I fully intend to comply with this policy realizing that I am personally responsible for intentional misuse or abuse of the State's communications and computer systems. I understand that the State of Delaware has no authority over non-state employees. However, all users must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources. If DTI learns of a possible inappropriate use, DTI will immediately notify the affiliate responsible, which must take immediate remedial action and inform DTI of its action. In instances where affiliates do not respond in a timely or reasonably appropriate manner, are "repeat offenders", or if criminal activity is suspected, DTI will work directly with the proper authorities, and follow their guidance in determining appropriate action. In an emergency, in order to prevent further possible unauthorized activity, DTI may temporarily disconnect the user or affiliate. If I have any questions about the policy, I understand that I need to ask my supervisor for clarification.

Name: _____

Signature (Required): _____

Organization: _____

Date: _____