Delaware State University

University Area(s) Responsible: Division of Technology and Information Systems; Office of Finance and Administration

Policy Number & Name: 8-07: Acceptable Use Policy

Approval Date: 7/11/11

Revisions: _____

Related Policies and Procedures: _____

A Message to all DSU Communications and Computer System Users

This document formalizes the University policy for employees, students as well as contractors and other "users" of the University's communications and computer systems. Each department may also choose to develop and enforce its own acceptable use policies to further restrict the use within its areas. This may be done only with the understanding that, should a conflict exist, the University Acceptable Use Policy (AUP) takes precedence over all local policies developed within the department 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 University from Hackers, viruses, data loss etc. The threat is real, as each month, DSU 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 Delaware State University business with integrity, respect, and prudent judgment. Each of us is responsible for upholding the Universities commitment to the highest standards of conduct.

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 department is 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 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 the Information Resource Manager (IRM), Information Security Officer (ISO), or Office of Human Resources for additional clarification of this policy.

Note the Following:

Applicability

Delaware State University's expectations for responsible use are applicable to all parties who use the Universities communications and computer systems on behalf of the University, including, but not limited to, its employees, consultants, in-house contractors, and other "users", either full or part time.

Limitations

This acceptable use policy does not address every expectation or condition regarding acceptable use. It does not substitute for other more specific University 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 2. We encourage Departments to have their users review the AUP annually. The signed acknowledgement statement must be maintained by the

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

Acceptable Use of Communications and Computer Systems

Delaware State University 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 DSU Communications and Computer Systems?

Delaware State University communications and computer systems are any equipment, hardware, software or networks (including wireless networks) owned, leased, provided or used by or on behalf of Delaware State University that store or transmit voice or non-voice data. This includes telephones, cellular/wireless telephones, voice mail, computers, e-mail, facsimiles, pagers, and University Intranet or Internet access (including when accessed through personally owned computers).

Note: Personally owned computers are not authorized on campus to do University Business. Also, when used at home for University Business, you must ensure that any University 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 University systems, including strong logon passwords 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 University standards contained in this section and other University policies regarding protecting data and information stored on these systems.

Unlawful and Inappropriate Use

Users are obligated to never use University systems (such as the Intranet or Internet) to engage in activities that are unlawful, violate University 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 Delaware State University's liability, embarrassment or loss of reputation.

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

Protection and Integrity of Data

Users must maintain the integrity of University Information and data stored on University 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, University 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 University Information or communications. Users should seek counsel from their supervisor, HR, or General Counsel for an opinion when in doubt. The protection of data and information applies to all electronic venues that the University might be using such as email, web applications, social media, etc.
- Protect data and information by not auto-forwarding University email to non-authorized individuals.

Unauthorized Network Devices

Faculty, staff, students or other non-University users (contractors/vendors) are not permitted to connect any device to the Delaware State University network unless authorized by the Delaware State University I/T Department. These devices include but are not limited to computers, servers, hubs, switches and or wireless access points. If anyone tries to use these devices on campus and any University personnel identify them, these devices will be removed by the Delaware State University I/T Department.

In order to prevent further possible unauthorized activity, Delaware State University may temporarily disconnect any device from the network.

If this is deemed necessary by the Delaware State University I/T Department, every effort will be made to inform the person prior to disconnection, and every effort will be made to reestablish the connection as soon as it is mutually agreed upon.

Delaware State University 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 Delaware State University.

Personal Use

While University 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 Delaware State University policies.
- Lead to inappropriate costs to the State. (Excessive personal surfing, Excessive long distance or International phone calls, utilizing streaming services for personal use such as listening to music or watching videos, and downloading of illegal music and video files are *specifically forbidden*.)

Virus Protection

Users must ensure all electronic media is checked , 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 **Help Desk**. DSU has purchased anti-virus software for all University PC's.

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 University Information or software of a third party that is stored, copied, or otherwise used on University systems is treated according to Delaware State University's standards regarding nonpublic University Information and applicable agreements and intellectual property restrictions.

Delaware State University Monitoring

University communications and computer systems, including, but not limited to, computer networks, data files, e-mail, voice, and voice mail, may be monitored and/or accessed by the University to ensure the integrity of the technology, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes.

Although the I/T Department does not randomly monitor message or network transactions, The University may without notification or approval, monitor, access and review any and all communications originating from Delaware State University or delivered to Delaware State University.

– Employees should have no expectation of privacy in regard to use of these services. This is in accordance with 19 Del. C. chapter 7,# 705. See Appendix 1

Use of E-Mail 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 web sites or materials.
- Chain Letters.
- Information related to religious materials, activities or causes, including inspirational messages, charitable solicitations unless sanctioned by Delaware State University.
- Gambling.
- Auction-related information or materials unless sanctioned by Delaware State University.
- 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 institutions, companies, or products.
- Large personal files containing large graphics materials, video or audio files (such as photographs, movies, 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 Delaware State University.
- Unauthorized or inappropriate mass distribution of communications.
- Intentional importation of viruses.

- Any other materials that would be improper under this policy or other Delaware State University.

Note: In order to perform their job duties (for example, network monitoring), specific Delaware State University 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 2 will be denied access to the Universities Communications and Computer Systems.

When Delaware State University learns of a possible inappropriate use, Delaware State University will take immediate remedial action. In instances where users do not respond in a timely or reasonably appropriate manner, are "repeat offenders", or if criminal activity is suspected, Delaware State University will work directly with the proper authorities, and follow their guidance in determining appropriate action.

Any inappropriate use of Delaware State University communications and computer systems may be grounds for discipline up to and including dismissal. Exempt employees shall be subject to appropriate discipline without recourse, except as provided by law.

Any determination of non-acceptable usage serious enough to require disconnection will be promptly communicated to HR, University General Counsel, by the Delaware State University IT Team.

Unauthorized activity or non-acceptable usage determined DSU may be subject to remedial action being taken in accordance with the acceptable use. Delaware State University 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.

Delaware State University 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.

Delaware State University 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 Delaware State University.

APPENDIX 1

§ 705. Notice of monitoring of telephone transmissions, electronic mail and Internet usage.

(a) As used in this section, "employer" includes any individual, corporation, partnership, firm or association with a place of business in Delaware and the State of Delaware or any agency or political subdivision thereof.

(b) No employer, nor any agent or any representative of any employer, shall monitor or otherwise intercept any telephone conversation or transmission, electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer either:

(1) Provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer-provided e-mail or Internet access services; or

(2) Has first given a 1-time notice to the employee of such monitoring or intercepting activity or policies. The notice required by this paragraph shall be in writing, in an electronic record, or in another electronic form and acknowledged by the employee either in writing or electronically.

The notice required by this subsection shall not apply to activities of any law enforcement officer acting under the order of a court issued pursuant to Chapter 24 of Title 11.

(c) Whoever violates this section shall be subject to a civil penalty of $100 for each such violation. A civil penalty claim may be filed in any court of competent jurisdiction.

(d) The provisions of this section shall not be deemed to be an exclusive remedy and shall not otherwise limit or bar any person from pursuing any other remedies available under any other law, state or federal statute, or the common law. The violations of this section by an employer shall not be admitted into evidence for the purpose of, or used as, a defense to criminal liability of any person in any Court in this State.

(e) The provisions of this section shall not apply to processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or Internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection.

APPENDIX 2

ACKNOWLEDGMENT STATEMENT

Delaware State University - Acceptable Use Policy

This is to certify that I have read and agree to abide by the guidelines set forth within the University 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 Delaware State University 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 Universities communications and computer systems. I understand that all users must agree to abide by all policies and standards promulgated by DSU as a condition of access and continued use of these resources. If DSU learns of a possible inappropriate use, DSU will immediately notify the department or user responsible, which must take immediate remedial action. In instances where departments or users do not respond in a timely or reasonably appropriate manner, are "repeat offenders", or if criminal activity is suspected, DSU will work directly with HR, University General Counsel, or the proper authorities, and follow their guidance in determining appropriate action. In an emergency, in order to prevent further possible unauthorized activity, DSU may temporarily disconnect the user, department, or building. If I have any questions about the policy, I understand that I need to ask my supervisor for clarification.

Name (Print) _____

Signature: _____

Dept / Phone: _____

Date: _____

Accepted by: (H/R) _____

Assigned Userid: (I/T) _____