11:02:04:00 Computing, Network and Communications Acceptable Use

Purpose:

The purpose of this policy is to outline the acceptable use of technology resources at Dyersburg State Community College. These rules are in place to protect the employees, students and the college. Inappropriate use exposes DSCC to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope:

This policy applies to employees, contractors, consultants, temporaries, other workers and students at Dyersburg State Community College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DSCC. This policy applies to all computing, network and communications resources provided by Dyersburg State Community College and to all users of these resources. Access to DSCC's information technology (IT) resources is a privilege. This privilege may be limited or revoked if an individual violates DSCC policies, TBR policies or state or federal laws. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, telecommunications equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Dyersburg State Community College. These systems are to be used for business or educational purposes in serving the interests of the institution, and of our students in the course of normal operations.

Policy:

3.1 General Use and Ownership

1. While DSCC's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the college's systems remains the property of DSCC. Because of the need to protect DSCC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to DSCC.
2. For security and network maintenance purposes, authorized individuals within DSCC may monitor equipment, systems and network traffic at any time.
3. DSCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4. Employees will only be allowed to enable one personally owned mobile device to connect to the DSCC email server and/or network. The use of this device should be for business related purposes only such as accessing e-mail, contacts or calendars.

3.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. All system level and user passwords should be changed quarterly.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
3. Use encryption of information in compliance with the Information Security policy.
4. All DSCC owned laptops used by faculty and staff must be encrypted.
5. Personal mobile devices should not be used to access the Enterprise Resource Planning system (currently Banner) of the college or any other system that contains personally identifiable information, bank account information or credit card information for students, employees, alumni or vendors of the college.
6. Postings by employees from a DSCC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DSCC, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the DSCC Internet/Intranet/Extranet, whether owned by the employee or DSCC, shall be continually running approved anti-virus software, if available, with a current signature database unless overridden by departmental or group policy.
8. Employees must exercise caution and good judgment when opening email attachments. Whether the sender is known to the user or not, these attachments may contain viruses, spyware and other malware.

3.3 Unacceptable Use of DSCC resources

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 DSCC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DSCC-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.

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 DSCC.
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 or movies, and the

installation of any copyrighted software for which DSCC 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, spyware, 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 a DSCC 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. 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, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Port scanning or security scanning is expressly prohibited unless prior notification to and approval of` the Vice President of Technology is made.
9. 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.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's computing session, via any means, locally or via the Internet/Intranet/Extranet.
13. Providing information about, or lists of, DSCC employees to parties outside DSCC.

Peer to Peer Software

1. The loading of peer to peer and other distributed file-sharing software on any computer or device owned by DSCC is prohibited.
2. Users found to have peer to peer and other distributed file-sharing software on any computer for which they have responsibility, will be reported to their supervisor, the appropriate Vice President and the President.
3. Current examples of peer to peer file and music sharing software includes BitTorrent clients (such as µ-Torrent, Tixati, Vuze/Azureus, etc.), Bearshare, Limewire, iMesh, and Morpheus.

Email and Communications Activities

Refer to DSCC E-mail Policy 11:01:04:00.

3.4 Acceptable Use of Social Media

1. Use of social media such as Facebook, Twitter, Foursquare, blogs, forums, wikis, podcasts and other interactive communication technology is permitted only for educational or work related purposes using DSCC resources.

2. Accounts or sites representing Dyersburg State Community College or any departments, divisions, or student organizations of DSCC on any social media must be requested and approved by the Vice President for Technology and the Director of Public Information.
3. Posts by employees with DSCC accounts or to DSCC sites, whether using DSCC's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.
4. Posts should be written in a professional and responsible manner, should not otherwise violate DSCC policy, and should not be detrimental to DSCC's or the Tennessee Board of Regent's best interests.
5. Employees are prohibited from revealing any DSCC confidential or sensitive information when engaged in posting or publishing to social media.
6. Employees shall not engage in any posts that may harm or tarnish the image, reputation and/or goodwill of DSCC and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when posting to an official DSCC site or otherwise engaging in any conduct prohibited by DSCC's Non-Discrimination and Anti-Harassment policy.

Compliance:

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

Definitions:

Blogging Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Peer to Peer Software program that share files with peers on a network usually by automatic discovery. These systems are frequently used for unlawful activities, such as sharing copyrighted material such as music and video.

Social Media Technology using web-based, mobile and/or other technology to provide interactive communication.

Spam Unauthorized and/or unsolicited electronic mass mailings.

Revision History:

Policy written April, 2011 by Vice President of Technology; approved by Administrative Council 04/29/2011.
Policy revised June, 2011; approved by Administrative. Council 06/21/2011.
Revision approved by Admin Council on April 29, 2016.

Updated language in reference to personal devices in July 2016 by Vice President for Technology in July Approved by Admin Council on July 29, 2016.
