Overview

Data, electronic file content, information systems, and computer systems at San Diego City College (SDCC) must be managed as valuable organizational resources.

The intention of this standard is not to impose restrictions that are contrary to SDCC's established culture of openness, trust, and integrity. SDCC is committed to protecting authorized users, partners, and the community from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Web-browsing, and File Transfer Protocol (FTP) are the property of SDCC and the San Diego Community College District (SDCCD).

These systems are to be used for business purposes in serving the interests of SDCC and of its administrators, faculty, staff, and students during normal operations.

Effective security is a team effort involving the participation and support of every SDCC employee, volunteer, and affiliate who deals with information and/or information systems.

It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

Purpose

The purpose of this standard is to outline the acceptable use of computer equipment at SDCC. These rules are in place to protect the authorized user and SDCC. Inappropriate use exposes SDCC to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This standard applies to the use of information, electronic and computing devices, and network resources to conduct SDCC business or interact with internal networks and business systems, whether owned or leased by SDCC, the employee, or a third party.

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at SDCC, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with SDCC policies and standards, local laws, and regulations.

Definitions

Information Systems: All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of administrative, instructional, research, or service activities.

Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Authorized User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

Extranet: An intranet that is partially accessible to authorized persons outside of a company or organization.

Standard Detail

Ownership of Electronic Files

All electronic files created, sent, received, or stored on SDCC owned, leased, or administered equipment or otherwise under the custody and control of SDCC are the property of SDCC.

Privacy

Electronic files created, sent, received, or stored on SDCC owned, leased, or administered equipment, or otherwise under the custody and control of SDCC are not private and may be accessed by SDCC IT employees at any time without knowledge of the user, sender, recipient, or owner.

Electronic file content may also be accessed by appropriate personnel in accordance with directives from Human Resources or the Chancellor.

General Use and Ownership

Access requests must be authorized and submitted from departmental supervisors for employees to gain access to computer systems. Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the corporate systems immediately become the property of SDCC. Because of the need to protect SDCC's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to SDCC.

For security and network maintenance purposes, authorized individuals within the SDCC IT Department may monitor equipment, systems, and network traffic at any time.

SDCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with district policies and standards.

SDCC reserves the right to remove any non-business-related software or files from any system.

Examples of non-business-related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.

Security and Proprietary Information

All mobile and computing devices that connect to the internal (non-public wi-fi) network must comply with this standard:

- System level and user level passwords must comply with the Password standard. Authorized users must not share their SDCC login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes.
- Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- Authorized users may access, use, or share SDCC proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.
- All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.
- All users must lockdown their PCs, laptops, and workstations by locking (control-alt-delete) when the host will be unattended for any amount of time. Employees must log-off, or restart (but not shut down) their PC after their shift.
- SDCC proprietary information stored on electronic and computing devices, whether owned or leased by SDCC, the employee, or a third party, remains the sole property of SDCC. All proprietary information must be protected through legal or technical means.
- All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of SDCC proprietary information to their immediate supervisor and/or the IT Department.
- All users must report any weaknesses in SDCC computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the IT Department.
- Users must not divulge dial-up or dial-back modem phone numbers to anyone without prior consent of the SDCC IT Department.
- Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

Unacceptable Use

Users may not intentionally access, create, store, or transmit material which SDCC may deem to be offensive, indecent, or obscene unless directly related to academic research.

Under no circumstances is an administrator, faculty, staff, or student of SDCC authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing SDCC-owned resources.

System and Network Activities

The following activities are prohibited by users, with no exceptions:

- 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 SDCC.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SDCC or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to IT.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others, including family and other household members when work is being done at home.
- Using a SDCC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Attempting to access any data, electronic content, or programs contained on SDCC systems for which they do not have authorization, explicit consent, or implicit need for their job duties.
- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of SDCC IT.
- Installing or using non-standard shareware or freeware software without SDCC IT approval.
- Installing, disconnecting, or moving any SDCC owned computer equipment and peripheral devices without prior consent of SDCC's IT Department.
- Purchasing software or hardware, for SDCC use, without prior IT compatibility review.
- Purposely engaging in activity that may;
    - degrade the performance of information systems;
    - deprive an authorized SDCC user access to a SDCC resource;
    - obtain extra resources beyond those allocated; or
    - circumvent SDCC computer security measures.
- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, SDCC users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on SDCC information systems. The SDCC IT Department is the only department authorized to perform these actions.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Access to the Internet at home, from a SDCC-owned computer, must adhere to all the same policies and standards that apply to use from within SDCC facilities. Authorized users must not allow family members or other non-authorized users to access SDCC computer systems. SDCC information systems must not be used for personal benefit.

Incidental Use

As a convenience to the SDCC user community, incidental use of information systems is permitted. The following restrictions apply:

- Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.
- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to SDCC approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to SDCC without prior approval of management.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, SDCC.
- Storage of personal email messages, voice messages, files, and documents within SDCC's information systems must be nominal.

All messages, files, and documents — including personal messages, files, and documents — located on SDCC information systems are owned by SDCC, may be subject to open records requests, and may be accessed in accordance with this standard.