Overview

Hardware and electronic media disposition is necessary at SDCC to ensure the proper disposition of all non-leased SDCC IT hardware and media capable of storing member information. Improper disposition can lead to potentially devastating fines and lawsuits, as well as possible irreparable brand damage.

Purpose

SDCC owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this standard. Where assets have not reached end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This standard will establish and define practices, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

SDCC's surplus or obsolete IT assets and resources (i.e., desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and SDCC's upgrade guidelines. All disposition procedures for retired IT assets must adhere to district approved methods.

Definitions

Beyond reasonable repair: Refers to all equipment whose condition requires fixing or refurbishing that is likely to cost as much or more than total replacement.

Chain of Custody (CoC): Refers to the chronological documentation of the custody, transportation, or storage of evidence to show it has not been tampered with prior to destruction.

Disposition: Refers to the reselling, reassignment, recycling, donating, or disposal of IT equipment through responsible, ethical, and environmentally sound means.

Non-leased: Refers to all IT assets that are the sole property of SDCC, that is, equipment not rented, leased, or borrowed from a third-party supplier or partner company.

Obsolete: Refers to all equipment that no longer meets requisite functionality.
Surplus: Refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

Policy Detail

The SDCC IT Department is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment. IT is also responsible for the chain of custody in acquiring credible documentation from contracted third parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations.

It is the responsibility of any employee of SDCC's IT Department, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the Hardware and Electronic Media Disposal Procedure. It is imperative that all dispositions are done appropriately, responsibly, and according to IT lifecycle standards, as well as with SDCC's resource planning in mind. Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)
- Printers
- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives / Flash memory
- Other portable storage devices

NIST SP800-88 Guidelines for Media Sanitation

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

Supplemental Guidance

- A single pass overwrite of magnetic or solid state media is recommended. While multiple overwrites can be performed, this does not provide any additional assurance that data has been irreversibly removed (see the National Institute for Standards and Technology Special Publication 800-88). It is important to note that a range of factors can impact the effectiveness and completeness of an overwrite operation. For example, some software may not be able to access all data on a hard drive, such as reallocated sectors resulting

from a drive fault. Reuse of electronic media outside of the organization is not recommended unless sanitization can be fully validated. If available, a firmware-based Secure Erase is recommended over a software-based overwrite. In situations where a third-party warranty or repair contract prohibits sanitization, a confidentiality and non-disclosure agreement should be put in place prior to making the electronic media available to the third-party.

- Media destruction should be performed in a manner that is consistent with techniques recommended by the National Institute of Standards and Technology (see Appendix A of Special Publication 800-88). Shredding and incineration are effective destruction techniques for most types of electronic media. The Information Security Officer recommends destroying electronic media through SDCC's Computer Recycling Program, which is managed by the district's IT department. In situations where a third-party warranty or repair contract prohibits destruction, a confidentiality and non-disclosure agreement should be put in place prior to making the Electronic Media available to the third-party.

- Common techniques for destroying institutional data in written or printed form include cross shredding or incineration. In situations where cross shredding or incineration are either not feasible or impractical, use of a third-party data destruction service may be appropriate. Reasonable effort should be made to track and inventory data sent to a third-party for destruction and evidence of destruction should be retained (e.g. Certificate of Destruction). In situations where documents are destroyed in large quantities or are collected and sent to a third-party for destruction, a secure trash receptacle should be leveraged to mitigate the risk of unauthorized access during the collection period. A confidentiality and non-disclosure agreement should also be put in place prior to sending any data to a third-party.