Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure establishes requirements to securely manage Information Technology (IT) assets and prevent data loss of organizational IT assets in the Washoe County School District (District).

DEFINITIONS

1. "Encryption" refers to a procedure used to convert data from its original format to an unreadable or unusable format to anyone without the tools or knowledge needed to reverse the process.

2. "IT asset" refers to anything (tangible or intangible) that has value to an organization, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both installed and physical instances), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards), as well as intellectual property (including software).

3. "Malware" refers to software of malicious intent such as viruses, worms, or spyware.

4. "Removable Media" refers to a portable device that can be connected to an information system (IS), computer, or network to provide reusable, readable and/or writeable data storage.

5. "Sanitization" refers to a process that renders access to target data on media infeasible. Clearing, purging, or physically destroying are actions that can be taken to sanitize.

PROCEDURE

1. All District employees have a responsibility to protect the confidentiality, integrity, and availability of District information that is collected, processed, transmitted, stored, or transmitted using IT assets whether they are District-owned or personal devices.

2. Responsibility for the proper care of IT assets is shared between District employees to which it has been assigned, District Departments, IT Service Providers, and the Office of Information Technology.

3. IT assets must be managed throughout their entire lifecycle to:

    a. Effectively track and manage IT assets;

    b. Optimize usage and workplace productivity;

    c. Standardize supported devices and configurations to offer efficiency gains through simplified technical support and maintenance requirements;

    d. Reduce waste; and

Ensure that IT assets are properly wiped of District data prior to reallocation or disposal.

4. IT Device Management Lifecycle:

    a. Plan. Align to target architecture and IT strategic plan.

    b. Acquire. Perform market research and negotiate agreements to maximize value.

    c. Deploy. Implement IT assets through standardized processes to ensure maximum usage and value.

    d. Manage. Implement and maintain supporting infrastructure and process to enhance productivity and customer satisfaction.

    e. Retire. Provide planned, orderly, and secure disposition of assets.

5. Centralized IT Asset Tracking:

    a. The Office of Information Technology must establish and maintain an accurate, detailed, and current inventory of all enterprise IT assets with the potential to store or process District data including devices connected to the District's network physically, virtually, remotely, and those hosted within cloud environments.

    b. IT assets must be centrally tracked and registered in the Enterprise Configuration Management Database (CMDB) as Configuration Items (CI).

    c. Each CI must include:

        i. Device hostname;

ii. Device Type (Workstation, Server, Mobile, Physical, Virtual, Container, Printer, etc.);

iii. Device make and model;

iv. Description;

v. Device Serial Number or unique identifiers;

vi. Asset Tag Number;

vii. Data Asset Owner;

viii. Assignee;

ix. Information Classification (if processing sensitive information);

x. Network addresses (if statically assigned or reserved)

xi. Hardware addresses;

xii. Department;

xiii. Location;

xiv. Relationships with other CI

xv. Whether the device is approved to connect to the District network; and

xvi. Purchasing Information;

- Budget Code;
- Purchase date;
- Received date; and
- Disposal date.

6. IT Asset Identification and Discovery:

   a. The Office of Information Technology may populate the CMDB by performing direct network and cloud infrastructure monitoring.

   b. Asset discovery may be performed against devices connected to the enterprise network through active scanning, passive discovery tools, and infrastructure service logging (Identity, Network Addressing, Mobile Device Management) on a regular basis.

c. In addition to District-owned IT assets, mobile and end-user devices connected to the District infrastructure or information resources may be registered in the CMDB due to their attempted or actual access of District information.

d. Devices connecting to the District enterprise network must be District-owned or controlled. The District requires the use of the Guest Wireless network by students, staff, visitors, and others using personal devices.

e. Unauthorized devices that introduce unacceptable risk through direct activities, misconfiguration, or outdated software may be removed from the network, denied from connecting remotely to District IT resources, or quarantined.

f. In instances where Departments have directly acquired District-owned IT assets, all users and Departments must report their assets to the Office of Information Technology for registration in the CMDB. District-owned assets that are not registered in the CMDB may be treated as unauthorized devices.

7. Asset Marking:

   a. All District-owned IT assets must have a District IT asset number assigned and mapped to the device's serial number or other unique identifier.

   b. When an asset is acquired, Office of Information Technology employees or appropriate designees must enter the assigned IT asset number into the CMDB.

   c. District-owned assets must be physically marked with District asset tags provided by the Office of Information Technology. If the device is too small to be physically tagged, it may be kept in a case which will be tagged.

8. Deployment and Management:

   a. Installations, service, and support performed by the Office of Information Technology must reference the asset tag and have an associated IT Work Order or ticket.

   b. All IT assets maintained in the CMDB must be located at a District facility or in the custody of an assigned user. Assignees must have a current and continuing relationship or employment status in the District. Assets must be transferred from users leaving the District prior to departure.

   c. District-owned IT Assets must:

i. Be enrolled in Enterprise IT Management tools controlled by the Office of Information Technology.

ii. Implement standardized system images and configurations using the Center for Internet Security (CIS) Benchmarks, wherever practicable.

iii. Be configured for least-privilege functionality, including disabling or uninstalling unnecessary services and software.

iv. Be configured for automated Operating Systems and installed Software updates and patching.

v. Have security software installed, including District-provided anti-malware software and log monitoring tools.

9. Device Security:

    a. Users must ensure IT assets are physically secured by storing devices in protected areas, such as locked desks or offices in District facilities.

    b. Users must not leave devices unattended in public areas.

    c. If a device containing District information is lost or stolen, the incident must be reported to the Office of Information Technology, IT Security Department immediately.

10. Retirement and Disposal:

    a. When assets have reached the end of their useful life or are no longer needed, they should be reallocated whenever practicable. Assets that cannot be reused must be securely retired and disposed of ("E-Waste").

    b. District IT assets must be sanitized or physically destroyed prior to disposal to ensure that the data stored on the devices is unrecoverable.

    c. Sanitization methods will differ based on the type of removable media. Media sanitization must occur in accordance with industry best practices, or the established recommendations published in NIST 800-88 r 1, "Guidelines for Media Sanitization."

    d. If the District outsources media sanitization and disposal to a third-party e-waste provider, the vendor must adhere to the District's established standards for media disposal. Third-party vendors must provide Certificates of "Sanitization" or "Destruction" including device serial numbers when disposing of removable media on behalf of the District.

11. Bring Your Own Device (BYOD):

    a. Bring Your Own Device (BYOD) is the act of using a personal computing device (computer, tablet, phone, etc.) for District business.

    b. Personally owned devices can improve user productivity and technology accessibility, but must be appropriately monitored, controlled, and appropriately restricted when accessing District IT resources.

    c. The District does not require employees to use personal equipment for District business.

    d. Access to District IT resources from personally owned devices may be revoked at any time.

    e. Users who wish to use a personal device for District business must:

        i. Register their device with the Office of Information Technology.

        ii. Use only software authorized by the Office of Information Technology that is configured with remote wiping capabilities.

        iii. Not store sensitive or confidential information on personally owned devices.

        iv. Destroy, remove, or return all data belonging to the District once they no longer have a need to access the information or their relationship with the District has ended.

        v. Only connect to District Guest network, never connect to the District internal network.

        vi. Notify the Office of Information Technology, IT Security Department immediately of any theft or loss of a personal device containing District data or applications.

    f. Users may receive limited IT support services for personal devices related to:

        i. Installation and support of approved District software resources; and

        ii. Troubleshooting network connection issues while on the District network.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:
    a. Board Policy 7205, Information Technology – Data Access; and
    b. Board Policy 7210, Information Technology Services and Operations.
2. This Administrative Procedure aligns and complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC), to include:
    a. NRS Chapter 603A, Security and Privacy of Personal Information.

REVISION HISTORY

Date	Revision	Modification
04/29/2024	v1	Adopted