Administrative Procedure 7229
INFORMATION TECHNOLOGY – APPROVED SOFTWARE

Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure establishes requirements for approved software on Washoe County School District (District) Information Technology Systems and provides standards that the District uses to mitigate information security risks associated with authorized software.

DEFINITIONS

1. "IT Ticketing System" refers to the system used to request support.
2. "Software" refers to a set of instructions, programs, or routines used to operate computers and execute specific tasks. This includes applications (apps), scripts, and programs that run on servers, workstations, and mobile devices (tablets/cell phones) such as database software, multimedia software, internet browsers, portable executables, browser extensions, and drivers, as well as hosted applications (Software as a Service (SAAS) "cloud-based" and System libraries.

PROCEDURE

1. Roles and Responsibilities:

   a. Software User

      i. Responsible for the business function that associated IT asset support.

      ii. Requests software approval and installation through the IT Ticketing System.

      iii. Reviews software approval list prior to use to determine approval status or documented exceptions.

b. IT Enterprise Services

   i. Installs, manages, and maintains systems and applications.

   ii. Prepares applications and packages them for distribution.

   iii. Administers configurations, policies, and user groups related to application deployment.

   iv. Removes unauthorized software from District IT systems.

c. IT User Services

   i. Provides end user support including installation and maintenance of approved software.

   ii. Troubleshoots failed software installations.

d. IT Security Department

   i. Maintains security software policy and enforcement mechanisms.

   ii. Implements approved security exclusions in support of approved business and educational software.

e. Chief Information Officer

   i. Oversees the District's IT implementation.

   ii. Ensures that software review and approval has been performed.

f. Office of Information Technology

   i. Maintains the District Configuration Management Database (CMDB).

   ii. Maintains and distributes a list of approved software ("Approved Software List").

iii. Maintains licensing information for software installed on District systems.

iv. Supports the authorized use of approved software through centralized deployment, configuration, and management.

2. Categories of Software:

a. Software may be related to a business function ("productivity software"), an educational tool used by teachers and/or students in the classroom ("Digital Learning Tools" or "Educational Software") or may be security software ("anti-malware" or "anti-virus").

b. Business or Productivity Software

i. Helps to accomplish the core missions of the District by improving or automating otherwise manual processes.

c. Educational or Digital Learning Tools Software

i. All software that may be used by teachers and/or students must be evaluated under the Digital Learning Tools (DLT) process to determine what student information is necessary to operate the system.

d. Security Software

i. Used to prevent unauthorized or malicious software ("malware") from being installed or executed on District IT systems.

ii. May need to be modified to support approved productivity or Digital Learning Tools software. Exclusions may be entered to support approved software.

3. Approved Software:

   a. Prior to installing or using software on District Information Systems, it must be approved through the Contract Review and Approval process as described in Administrative Regulation 3322 for productivity software or through the Digital Learning Tools approval process when the software is intended to be used with students.

   b. The Office of Information Technology reviews and either approves or rejects software based on software functionality, as well as IT network, host, or security impacts.

   c. Other District departments, including the Business and Legal Offices, may perform supplementary reviews to determine whether District personnel privacy, financial, licensing or usage agreements are unfavorable. Software with unfavorable terms may be disabled or uninstalled at any time.

   d. Upon learning of unauthorized software, the IT Department may implement technical measures to isolate, restrict, or remote use of unauthorized software from the District Information Systems.

   e. All approved software must be:

      i. Tracked in the Enterprise Configuration Management Database ("CMDB");

      ii. Appropriately licensed for use;

      iii. Regularly updated to the most recent major version to address security and stability flaws;

      iv. Regularly evaluated for technical vulnerabilities including ones disclosed by the vendor or software developer and third parties;

v. Securely configured using the "least privilege" model. For instance, services that are installed by the software, but are unrelated to its core functions must be disabled or uninstalled;

vi. Centrally managed by the Office of Information Technology whenever practicable;

vii. Prevented from subverting security controls including any actions that disrupt or degrade the confidentiality, integrity, or availability of information resources.

4. Configuration Management Database ("CMDB") and the Approved Software List:

a. The Office of Information Technology must establish and maintain an accurate, detailed, and current inventory of all enterprise IT assets including software.

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

c. Each CI must include:

i. Software Title;

ii. Software Category;

iii. Description;

iv. Licensing;

v. Publisher;

vi. Initial Installation/Use Date;

vii. The business purpose;

viii. Whether or not the software is authorized; and

ix. Where appropriate:

- The originating URL;
- App Store;

- Versions installed or approved;
- Deployment Mechanism (Local Installation or Software Packaging);
- Decommission Date;
- Ticket Number;
- Information Classification (if processing sensitive information);
- Audience (Department and Location);
- Relationships with other Configuration Items (CI); and
- Purchasing Information
    - Budget Code;
    - Purchase date;
    - Received date; and
    - Disposal date.

d. Software inventory tools may be used to automate the discovery and documentation of installed software on District Information Systems including those that were introduced through alternative processes and workflows.

e. The Office of Information Technology may regularly update the published "Approved Software List" to provide users with a comprehensive list of approved software found on the Office of Information Technology's website.

5. Software Maintenance:

a. Software must be regularly maintained using vendor-provided updates or patches. In some cases, software may need to be reconfigured to mitigate the impact of vulnerabilities.

b. Software maintenance may be performed differently based on how the software was initially installed and the overarching system management strategy.

c. Software Management:

i. Local Installation

- Standalone, individual installations must be performed by privileged users (i.e. Administrators) of systems through a manual or automated process.

- This software is largely unmanaged by centralized IT services and must be managed directly by the user.

ii. Managed Installation

- Software may be packaged to allow standard users to perform self-service installations.

- Software management may be performed by the Office of Information technology.

d. Security Software Exclusions:

i. Approved software may require modifications to security software or configurations ("Exclusions") to enable installation or execution.

ii. The IT Security Department is responsible for evaluating and implementing proposed exclusions based on the relative risk to the computing environment.

iii. Implementing exclusions may require identifying and establishing compensatory controls to ensure that unacceptable risk is not introduced.

e. Software Renewal:

   i. Software approvals must be reviewed biannually or whenever a major change has occurred in the operating environment or software.

   ii. Major changes may include the deprecation or introduction of other technologies across industry, architectural changes to the District network, or identification of software vulnerabilities.

6. Exceptions

   a. Exceptions may be made to this Administrative Procedure regarding the installation of unapproved software for specific workloads, projects, or academic needs. Exceptions will be made on a case-by-case basis based on the needs of the District.

   b. Students performing coursework directly related to District-approved Career and Technical Education (CTE) programs within specific technical environments or labs may need to access prohibited software.

   c. The IT Security Department will handle and document exceptions in the IT Ticketing System.

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. Administrative Regulation 7211, Responsible Use and Internet Safety.

REVISION HISTORY

Date	Revision	Modification
05/02/2024	v1	Adopted