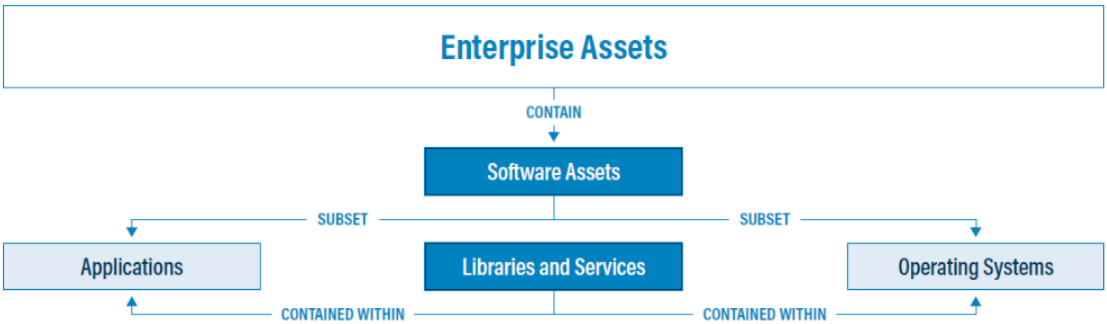
SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **SOFTWARE ASSET MANAGEMENT**	Procedure 8.19.01

I. PROCEDURE STATEMENT

The IT Division ("IT") is responsible for all software asset management functions. This information is relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them.

II. DEFINITIONS

Software assets include both operating systems and applications:



Operating system: System software on enterprise assets that manages computer hardware and software resources, and provides common services for programs. Operating systems are considered a software asset and can be single- and multi-tasking, single- and multi-user, distributed, templated, embedded, real-time, and library.

Application: A program, or group of programs, hosted on enterprise assets and designed for end users. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications.

Additionally, there are multiple components that make up applications and operating systems, including services and libraries.

Service: Refers to a software functionality or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations. Services provide a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and based on the identity of the requestor per the enterprise's usage policies.

Library: Pre-written code, classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.

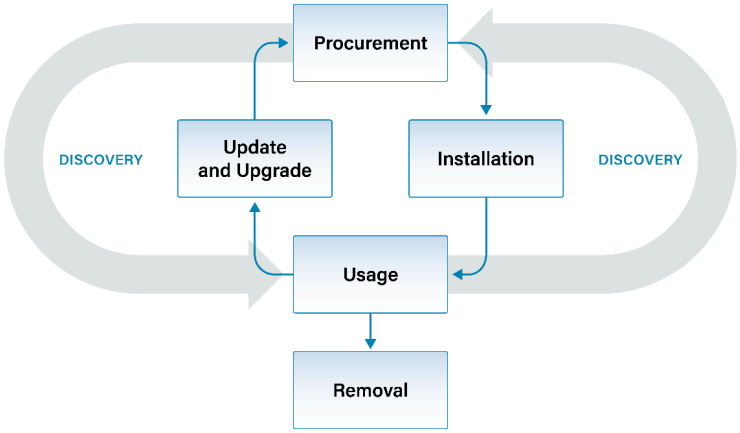
There are also several different types of software. The definitions revolve around the software owner, cost, and the ability to modify and redistribute the code. The following provides general definitions for different software types:

- **Free software:** Completely free to download, modify, distribute, and use software.
- **Freeware:** No-cost software that often includes a limited license to specific groups of users (e.g., students). Modification of source code is generally prohibited.
- **Open source:** Free software for download and use, but the license will dictate stipulations for modification and redistribution.
- **Commercial off the Shelf (COTS) software:** Software that is publicly available for purchase. Patrons are generally not authorized to modify the software.
- **Internally developed applications:** Software applications created and maintained by an enterprise and their contractors. The enterprise generally owns all rights save for any licenses used in development stipulating otherwise.
- **Shareware:** Often a type of software offered with a time-limited license, and potentially limited feature sets. Full versions are made available for purchase.
- **Scripts (e.g., PowerShell, Bash, Python):** A program that provides a series of instructions to the operating system, typically to accomplish a series of more basic tasks.

III. SOFTWARE ASSET MANAGEMENT LIFECYCLE

In order to protect a network and its assets, an enterprise must first know what software is on a network. In addition, many other security controls are dependent on the software asset inventory, such as secure configurations, account management, access control, and more.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **SOFTWARE ASSET MANAGEMENT**	Procedure 8.19.01



Procurement – Acquiring new software from software vendors and managing software licenses.

Installation – Deploying new software products to employee assets, to include phones, tablets, desktops, servers, and cloud infrastructure.

Discovery – The identification of software by actively searching systems connected to the enterprise network.

Usage – The authorized use of approved software by employees.

Update and Upgrade – Applying minor software patches or replacing a software asset with new functionality.

Removal – Deleting or retiring software from enterprise assets.

IV. PROCUREMENT

A. Only individuals from IT are approved to procure software.
B. IT must maintain a list of approved software vendors.
C. Software must only be purchased from vendors on the approved software list.

V. INSTALLATION

A. Any software installed on enterprise assets, alongside other relevant information within the software asset, must be recorded within the software inventory. This must include:
    1. Title of software
    2. Developer or publisher of software
    3. Date of acquisition
    4. Date of installation
    5. Duration of usage

6. Business purpose
7. App Store(s)
8. Version(s)
9. Uniform Resource Locator (URL)
10. Deployment mechanism
11. End-of-support (EoS) date, if known
12. End-of-life (EoL) date, if known
13. Any relevant licensing information
14. Decommission date

B. IT must verify the software asset inventory every six months, or more frequently as needed.
C. Only software that has been approved by IT may be installed.
D. Only cloud services that have been approved by IT may be used within the enterprise.
E. Mobile devices may only obtain software from IT approved sources.

VI. USAGE

In general, refer to the POLICY 8.02.01 *Computer Resources, Internet and Network Acceptable Use Policy*.

VII. DISCOVERY

A. IT must review all software installed on enterprise assets on a monthly basis.
    1. All installed software on enterprise assets must be reported to IT on a regular basis.
    2. All newly discovered software must be checked against the list of approved software in the software asset inventory.
B. Identified software not included within this inventory must be investigated as the software may be unauthorized.
    1. Assets containing unauthorized software must be removed from the network unless temporary access is granted by the IT business unit.
    2. The presence of unauthorized software must be properly investigated.
    3. All newly discovered (authorized) software must be added to the software inventory.
    4. Unauthorized software must be removed from use on enterprise assets or receive a documented exception.

VIII. UPDATE AND UPGRADE

A. All updates and upgrades must be approved by IT prior to installation. IT configuring a device for automatic updates, or directing users to do so, constitutes a tacit approval.

IX. REMOVAL

A. Software to be decommissioned must be removed from all enterprise assets.
B. Assets containing retired software must be protected with additional defensive mitigations, such as removal from the network or isolation.
C. IT must make a copy of the user data as needed.

D. Ensure that any retired software did not store data in other servers or cloud infrastructure not owned by the enterprise.

LEGAL REFERENCES:

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Control 2 (Inventory and Control of Software Assets)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Adopted: September 2025

Revised: N/A