Collin College Information Technology Services (CC-TS)
Desktop Security ISP:

PURPOSE:

The purpose of the Desktop Security ISP is to manage and secure Collin College computers and the network, reducing the risk of internal security attacks and the liability associated with unrestricted access and unlicensed software.

SCOPE:

The CC Desktop Security ISP applies to any data owner, data custodian, system administrator and CC user that utilizes CC desktops or mobile devices.

STATEMENT:

1. End users cannot self-install software. Standardized OS-specific gold images will be secured. If an end user requires software that is not included on a standard gold image, CC-TS must conduct a review of the software security, licensing, and business necessity before installing said software.
    a. This review must be approved by the Technology Services Technology Specialist assigned to the specific request, their direct supervisor, and a representative from the Security Department.
    b. Once a specific program has passed review, it may be added to an allow-list maintained by Technology Services to expedite software package installation in the future.
        i. This allow-list must be reviewed annually to ensure that no programs have become vulnerable to threats or gone out of support/end of life.

2. Endpoints must be classified in the following fashion and applied on a case-by-case basis.
    a. High Risk
        i. High Risk endpoints are machines that contain sensitive data on them that could potentially be lost without proper controls. Examples include but are not limited to:
            1. Laptops/tablets that leave college premises.
            2. Desktops or other machines that handle financial, PII, criminal, or other sensitive data. Departments or users that may fall under these categories include:
                a. Police Department.
                b. Human Resources.
                c. Financial Department.
                d. C-Suite executives and administrators.
                e. VP/Provosts and administrators.
        ii. High Risk endpoints must be secured with the following software (or equivalent) packages:
            1. SecureWorks Taegis (Red Cloak)

            2. Bit Locker Device Encryption
            3. System Center Configuration Center (SCCM)

    b. Moderate Risk
        i. Moderate Risk endpoints are machines that may potentially contain sensitive data but aren’t as necessary to secure data storage. Examples include but are not limited to:
            1. System administrators.
            2. Collin College Technology Services machines that have users with local administrator access.
            3. Servers that contain sensitive information.
        ii. Moderate Risk endpoints must be secured with the following software (or equivalent) packages:
            1. SecureWorks Taegis (Red Cloak)
            2. System Center Configuration Center (SCCM)

    c. Low/No Risk
        i. Low or No Risk endpoints are machines that do not require any controls to secure them as there is no sensitive data present. Examples include:
            1. Computer lab desktops.
            2. Student computers that stay on campus.
            3. Staff or faculty machines that do not have local administrator privileges.
        ii. Security controls are not necessary on Low or No Risk endpoints.

3. Anti-virus software with up-to-date virus definitions must be included and maintained on the Technology Service’s gold images as part of the standard software package.
    a. Anti-virus software must be approved and reviewed annually by the Security Department.

4. The OS of all CC machines must be, at a minimum, upgraded quarterly to account for critical security updates. The Security Department retains the right to recommend earlier upgrades if significant threats are posed to the integrity of the network and infrastructure.

5. Endpoints or endpoint peripherals must be set to require a password or re-authentication after a period of inactivity.

DEFINITIONS:

Data Owner(s): A Data Owner is a Collin College employee designated as accountable for specific institutional data. The Data Owner has administrative control over the dataset and is usually the most senior divisional officer. Data Owners are defined for the purposes of these ISPs, but Collin College remains the owner of data maintained, stored, or transmitted on and through CC's information technology resources.

Data Custodian: A Data Custodian is a Collin College employee who has operational or technical responsibility for institutional data. This person usually has administrative or root equivalent access to the data and is accountable to the Data Owner.

System Administrator: A System Administrator is a CC-Technology Services employee responsible for the installation, maintenance, and management of physical college-owned endpoints within the CC infrastructure.

End User: A (end) user is defined in NIST 800-66 as a person or entity with authorized access.

Secured: A term used for a CC-owned endpoint that allows a standard end user to perform usual tasks on said endpoint without the ability to install software.

Gold Image: An archetypal version of a cloned disk that is to be used as the standard template for all endpoints at a campus that includes software packages most required by faculty and staff.

Period of Inactivity: To be determined by individual departments, but length is not to exceed 15 minutes.

Implementation Information

Review Frequency:	Annually
Responsible Person:	CIO/IRM
Approved By:	Abe Johnson, Ed. D.
Approval Date:	3/19/2024

Revision History

Version:	Date:	Description:
1.0	3/19/2024	Initial document