Information Security Standard

Distributed IT

Initially Approved: March 9, 2023
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This information security standard operates under University Policy 117 Information Security. Additionally, Policy 1400.1 in the UNC Policy Manual requires "Demonstration of a comprehensive information technology governance program that encompasses both centralized IT and distributed IT consistent with the framework, principles, and guidelines." Therefore, it is imperative that WCU employees that are included under WCU's definition of Distributed IT are aware of, and comply with, established policies, standards and procedures related to IT.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to all University workforce members that fall under the definition of Distributed IT.

III. DEFINITIONS

a. "Distributed IT" shall mean non-Division of IT Employees who are managing endpoints and/or servers; or system administrators of hosted applications with Red or Orange data which are not part of WCU's Single Sign-on (SSO) authentication system.

b. "Managing endpoints" shall mean routinely installing software, imaging, or configuring endpoint devices as part of normal job duties.

c. "Managing servers" shall mean having administrator privileges on a system which is accessed by multiple users or otherwise available via public network access.

IV. DISTRIBUTED IT STANDARD

1. For owners of applications that house Red or Orange data and do not use WCU's SSO system for authentication, access re-certification must be done twice per year rather than once.

2. Non-Division of IT employees who are managing endpoints and/or servers:

    a. Must comply with the consolidated software inventory process and software purchasing policies;
    b. Must participate on the IT Liaisons Committee;
    c. Must not set up an Internet-accessible web server or IoT device without IT involvement;
    d. Must request and use a separate account for doing work on applications or servers that require elevated permissions;
    e. Must ensure that university data on servers is backed up;
    f. Must not house Red or Orange data on departmental servers; and
    g. Must attest to reading and understanding the following IT standards and procedures:

        i. Data Handling Procedures
        ii. Media Handling and Disposal Standard
        iii. Controls Against Malicious Software Standard
        iv. Information Security Incident Management Standard
        v. Network Authentication and Authorization Standard
        vi. Internet of Things Standard

3. Re-certifications and/or attestations will be requested from the IT Division in conjunction with other similar processes.

V. REVIEW

This standard will be reviewed periodically and updated as necessary.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)
University Policy 117 Information Security