Information Security Standard

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

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.

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

a. “Distributed IT” shall mean non-Division of IT Employees who are managing endpoints and/or servers; or system administrators O[P03list)(e)8n ppichancnsd id

anag(n)-4( )]TETQ

he ǫ ᾳ̃ DŽ ɢ r ľ Ōe ʿ ta ˧ ľ R ك hi ŋ h ľ no ˥ ľ ᾳ̃ ˈ W 3 U’ ŭ ˜ in ℷ le

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