1. No individual or office may connect a device to the WCU data network that provides unauthorized users access to the network or provides unauthorized IP addresses for users.
2. IT has the right to monitor WCU networks and limit network capacity, or disable, network connections that are adversely impacting the security or availability of IT resources.

V. Responsibilities

It is the responsibility of all faculty and staff to follow this information security standard. Failure to do so may result in the device being disabled on the network and possible disciplinary action.

It is the responsibility of the IT Division to enforce this standard.

VI. Exceptions

Exceptions to this standard must be approved by the CIO or their designee and include compensating controls that reduce the risk of not following this standard.

VII. References

International Standards Organization (ISO/IEC 27002:2022, Clause 8 Technological Controls)

University Policy 117 Information Security

University Policy 95 Data Network Security and Access Control