Information Security Standard 13.1a

Internet of Things Standard
Initially Approved: June 9, 2020
Administering Office: Office of the CIO

I. Standard Statement

This standard operates under University Policy 117 Information Security. The ever-growing prevalence of non-standard endpoint devices being connected to the WCU network has the potential to threaten the availability and security of information technology resources. To minimize this risk, a standard is required for connecting and maintaining Internet of Things (IoT) devices regardless of the potential adverse impact to their functionality.

II. Scope and Application

This standard applies to network connected devices that do not fall under the definition of "endpoint device" as given below.

This standard does not apply to devices connected to a ResNet wired port or the student and guest wireless networks.

III. Definitions

"Internet of Things*"** and ***"IoT Devices" generally mean computing devices that can transfer data over a network without human input, and it's not a computing device that serves as a means for a human to access the Internet (e.g., audio-visual equipment, appliances, lab equipment, smart devices, etc.)
"Endpoint device" shall mean an information technology (IT) device that includes, but is not limited to, a desktop, laptop, notebook, tablet, or smartphone that is generally used by a human to connect to the Internet.

IV. IoT Standard

a. The connection of an IoT device to the WCU network requires a ticket be submitted to the IT Division and the request fulfilled by IT staff
b. IoT devices shall be segregated on the network from the WCU Faculty/Staff VLAN(s)
c. IoT devices that have a user interface will always have any default or pre-configured user accounts either disabled or have the passwords changed
d. Owners of IoT devices will routinely check for and apply security patches
e. Per University Policy 95 Data Network Security and Access Control:

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, 13.1, Network security management)

University Policy 117 Information Security

University Policy 95 Data Network Security and Access Control