Information Technology Services
Internet of Things Standard

Effective: April 10, 2022
Next Review Date: April 10, 2024

Standard Statement

This standard ensures the security of Tarleton infrastructure by proactively managing Internet of Things (IoT) devices.

Reason for Standard

This standard ensures the confidentiality, integrity, and availability of the University's information resources by regulating the use and network connectivity of (IoT) devices. Adhering to this standard enables the University to reduce or eliminate potential exploitation of IoT technology.

Definitions

Internet of Things (IoT) – Physical objects that may be user or industrial devices that are connected to the internet and are embedded with sensors, controllers, software and other technologies for the purpose of connecting and exchanging data with other devices and systems

MAC – Media Access Control. A unique hardware identification number that identifies each device on the network

PAN – Personal Area Network. Provides communication between devices and connection to higher level networks

SSID – Service Set Identifier. The name assigned to a Wi-Fi (wireless) network

TAC 202 – Texas Administrative Code 202. Outlines the minimum information security and cybersecurity responsibilities and roles at Texas state agencies and institutions of higher education

UPnP – Universal Plug and Play. Network protocols that allow networked devices such as wireless access points, printers, and laptops to discover each other's presence on the network and to establish functional network services

Standards and Responsibilities

IoT Security

1. IoT devices must connected to a specific segregated and controlled network segment
2. Default credentials must be changed
3. Passwords must adhere to Tarleton's password policy
4. If possible, disable the administrator account and create a custom admin account. The custom account name should not reflect administrator rights (Example: admin, adm, administrator, superuser)
5. The administrator account should only be used for admin functions and not standard operations
6. All IoT devices should be updated as patches are released by the vendor
7. UPnP connections are not allowed on Tarleton's network
8. If possible, do not use MAC-based authentication
9. Disable PAN network capability if it is not required for functionality
10. Disable Wi-Fi SSID broadcasting or any feature that allows for Wi-Fi network broadcasting
11. Disable any unused interfaces such as the ability to be used as a hub or bridge
12. Tarleton's Information and Technology Services staff reserve the right to remove any IoT device from the University's network if network traffic received by or transmitted from the device is a threat to the University's digital landscape.
13. IoT devices that must adhere to this standard also include:
    a. Non-Tarleton devices owned by individuals or departments
    b. Devices that only require internet access for functionality
    c. Non-enterprise or consumer grade devices that are maintained by vendors

d. Non-enterprise or consumer grade devices that are not maintained

e. Devices with limited firmware and software support including limited or no updates

f. Devices with limited security capabilities. These devices may focus on functionality and not security.

Exceptions

Based on risk management considerations and business functions, the resource owner may request to exclude certain protection measures mandated by a control in favor of an alternate mitigation. To submit an exception request for any I.T. policy, complete the online Information Technology Policy Exception Request Form. Any exceptions shall be approved, justified, and documented in accordance with TAC 202.

Related Statutes, Policies, or Requirements

SAP 29.01.03.T0.01 Information Resources – Acceptable Use

Tarleton Security Control Standards Catalog:

AC-6 Least Privilege
AC-18 Wireless Access
CM-1 Configuration Management Policy and Procedures
IA-5 Authenticator Management
RA-5 Vulnerability Scanning
SA-22 Unsupported Components
SI-2 Flaw Remediation

Contact Office

Information Technology Services
Information Security Officer
(254) 968-9160