THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: SC-006-Internet Of Things Security	
Version 1	Effective Date: 05/31/2021

Responsible Office: Office of Cybersecurity	Last Review: 06/02/2021 Next Review: 06/02/2023
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To ensure the confidentiality, integrity, and availability of the University's IT Resources by regulating the controlled use of Internet of Things (IoT) devices and connecting them to the appropriate University network.

Scope

This IT standard, and all standards referenced herein, shall apply to all members of the University community, including faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions

IT Resources - Computing, networking, communications, applications, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

Internet of Things - Physical objects (e.g., vehicles, appliances, lab or medical equipment and other items embedded with electronics, software, sensors, actuators) that communicate, sense, or interact with their internal states or the external environment via network connectivity.

Standard

1. In support of University functions, the Faculty/Staff must make an official request to use an IoT device or collection of devices using the Internet of Things Service Request from the ITS Service Catalog.
2. Faculty/Staff IoT device requests must be reviewed and connected to the appropriate controlled network segment.

3. University owned IoT devices must adhere to NISTIR 8259A IoT Cybersecurity Capability Core Baseline.
4. IoT devices must comply with all University information security standards such as, but not limited to, Network Security, Access Control, Data & System Classification, Vulnerability Management, and Password Management.
5. IoT networks must be monitored to identify abnormal traffic and emergent threats.

References

1. RM-002-Vulnerability Management
2. SC-001-Network Security
3. IoT Device Cybersecurity Capability Core Baseline (nist.gov)
4. Internet of Things Service Request Form