Title:	Internet of Things (IoT) Device Connection Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:			
Related Policies or Procedures:	EWU 203-01: Information Security EWU 901-02: Appropriate Use of University Resources		

History

Revision Number:	Change:	Date:
1.0	Initial version	8/18/2025

A. Purpose

The purpose of this procedure is to establish a secure and stable method for connecting Internet of Things (IoT) devices to the university network. By placing these devices on a separate, segmented IoT network, we can protect the integrity of our main Wi-Fi and wired networks, minimize security risks, and prevent signal interference that could disrupt essential academic and administrative operations. This process ensures that all devices comply with our institutional security policies and are managed effectively.

B. Definitions

Internet of Things (IoT) Device: A physical object or "thing" embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Segmented IoT Network: A dedicated, isolated network specifically designed to host IoT devices, separating their traffic from the primary academic and administrative networks to enhance security and prevent interference.

C. Procedure

To request and authorize the connection of an IoT device, please follow these steps:

1. **Submit a Request:** The faculty or staff member must submit a formal request to the IT department. The request must include the following information:
    - The user's name, department, and contact information.
    - A detailed description of the IoT device (make, model, serial number).
    - The purpose and function of the device.
    - The physical location where the device will be used.
    - Information on the device's security and maintenance capabilities, including its ability to receive software updates.

2. **Review and Approval:** The IT department will review the request based on a set of criteria designed to ensure network security and stability. This review process may include a security scan of the device and a physical inspection. The IT department will inform the user whether the request has been approved or denied.
3. **Network Placement:** If the device is approved, the IT department will provide instructions for its connection to the designated segmented IoT network. This network is isolated from the main campus network, providing an additional layer of security. The device must be configured to connect only to this specific network. The IT department will not approve connections to the main campus Wi-Fi for these devices.

Criteria for Denial

Requests for device connections may be denied for the following reasons:

- **Interference with Wi-Fi Signals:** Devices that operate on frequencies or in a manner that could interfere with the existing Wi-Fi network may not be approved.
- **Specific Consumer IoT Devices:** Devices designed for smart home, personal security, or recreational use (e.g., smart speakers, smart locks, home security cameras, video streaming sticks) are generally not approved for the university network due to their varying security standards and potential for unauthorized data collection.
- **Limited Security or Maintenance:** Devices that lack the ability to be patched or updated, have known security vulnerabilities, or have limited security features will not be approved. This ensures that every device on our network can be properly secured and maintained.

User Responsibilities

The faculty or staff member is responsible for ensuring the ongoing security and maintenance of their approved device. This includes installing any software updates provided by the manufacturer and promptly notifying the IT department of any changes in the device's function or location.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.

D. Other Information