Industrial Internet of Things (IIoT)

The connected world is growing at an exponential rate. The Internet of Things (IoT) goes beyond computers, tablets and phones and extends into internet connected cameras, HVAC systems, lawn sensors, energy consumption monitoring devices as well as any other device that connects to the network. This administrative regulation aims to create visibility of IIoT devices and adapt the overall security posture to accommodate and secure the devices along with its data and is in accordance with AR 0440.1. A partnership and common goal between Technology Services, Facilities Management, Purchasing, and other Fresno Unified departments as required.

IIoT devices provides data for analytics, ability to monitor and control systems remotely, and to provide central security to remote locations. With the rapid increase of IIoT devices and their operating environment they have become a popular target for hackers and people wanting to exploit vulnerabilities.

The intent is to ensure that quality service levels are maintained for end users, prevent inappropriate network congestion, and avoid over burdening Fresno Unified staff tasked with installing, maintaining and monitoring IIoT devices. This regulation along with Standards and Practices are to be reviewed at least annually. The use of IIoT devices is also governed by the District's Acceptable Use Policy (AUP).

It is imperative that Fresno Unified protect these devices with the same rigor as other endpoints on the network. Implementation of this regulation will establish a baseline of security that will protect: data privacy and integrity, the network environment and IIoT hardware.

IIoT devices are usually IP addressable end points or controller systems that utilizes the IoT framework of Edge processing coupled with either a web, cloud or app interface. Industrial Internet of Things (IIoT) is differentiated from consumer IoT due to the intended enterprise use, which include building environmental controls systems, security cameras, lawn maintenance sensors, energy consumption devices, etc. This regulation does not cover consumer IoT devices such as smart watches, health monitors, or devices connected under Bring Your Own Device (BYOD).

Inventory and Maintenance

All Fresno Unified IIoT devices are the responsibility of the approving department and tasked with device maintenance, physical security and administration once in operation. As the number of connected IoT devices grow an inventory with the following attributes is necessary for effective management:

1) Device Type
2) Purpose
3) Manufacturer
a) Model
b) Software Version (if applicable)
4) Location
5) Operational Group Owner
6) Configuration Notes

As devices reach end of life they must be retired under the same regulation of other Information Technology hardware.

The department approving the IIoT device will be considered the device "*owner"* and is responsible for monitoring device activity and device maintenance, which may include applying system/device patches when appropriate. Critical system/device patches need to be completed in a timely manner.
The operating environment, network (bandwidth and density) and other conditions need to be considered prior to purchase to ensure devices purchased are maximized to their fullest potential. As technology becomes increasingly embedded in throughout the enterprise, interdepartmental communication becomes ever more important. The landscape of the enterprise and interoperability should be considered during purchase and meet the minimum level of security standards and configurability.

Network and Security

Devices that connect to the network and/or devices that have internet connectivity must be secured in accordance to networking best practices. It is imperative to protect other Fresno Unified systems and maintain availability, integrity and confidentiality of those systems as well provide services for IIoT. Request for an exception to the regulation must be provided to the CTO in writing for review.

1. Authorization
a. IIoT devices can only be accessed by authorized personnel
b. Configuration can only be done by authorized personnel
c. Authorization lists provided to IT and reviewed quarterly by operational owner for accuracy
2. IIoT devices need to be connected to a segmented network (physical or virtual). This is to ensure network security and quarantining potential harmful traffic without interfering with device intended usage.
3. Devices must be configurable to:
a. Change any default passwords
b. Devices and service accounts need to be configured to use Least network privilege
4. Device Interfaces and Network Services
a. The vendor if using or providing a cloud service or local web server must encrypt data while at rest and in transit. The service provider must use industry standard security processes and procedures and not share data with third parties without prior written consent.
b. If the device uses a mobile app to report data or as remote control the app must use a secure connection and standard encryption for data on the device and while in transit. The service provider must use industry standard security processes and procedures and not share data with third parties without prior written consent. The app shouldn't save logon information longer than appropriate.
5. Physical Security
a. IIoT devices need to be physically secured to prevent loss or tampering.
b. Lost or stolen devices must be reported to Technology Services immediately

Standards and Practices

1. Devices that use Authentication/Authorization when connecting to Fresno Unified network will have preference.
2. Device Software/Firmware - If the device vendor offers software or firmware that is upgradable or offer security patches they need to be applied in a timely manner. Testing on a single device if a manual upgrade and practical. Automated updates should be turned on, unless a proper business case is presented otherwise.
3. IIoT devices should be able to function on current hardware and operating systems that is supported by the district.
4. Authorization access is documented and through business process with timely de-authorization of staff as needed.

5. Preference of 5ghz wireless devices, minimum performance requirement established during acquisition based on current network landscape and needs.

Regulation FRESNO UNIFIED SCHOOL DISTRICT
Approved: May 4, 2017 Fresno, California