**University of Alabama at Birmingham**

**INTERNET OF THINGS (IoT) SECURITY RULE**

Approved and Implemented: September 20, 2019

Reviewed/Updated: February 12, 2021

**Related Policies, Procedures, and Resources**

[Data Protection and Security Policy](http://www.uab.edu/it/home/component/k2/item/822-data-protection-and-security-policy)

[Data Access Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000789.aspx)

[Acceptable Use Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000004.aspx)

[Data Protection Rule](http://www.uab.edu/it/home/component/k2/item/818-data-protection-rule)

**1.0 Introduction**

Securing an Internet of Things (IoT) infrastructure requires a rigorous security-in-depth strategy. By taking a proactive approach to managing IoT devices, the university is able to reduce or eliminate the potential for exploitation and prevent the excessive time, effort, and potential costs that often result when responding to an exploitation after it has occurred.

**2.0 Scope and Applicability**

All IoT devices that reside on the UAB network (wired or wireless) must be proactively managed and adhere to the university’s IoT security strategy.

**3.0 IoT Device Security**

1. Default credentials for any IoT device/component must be changed, and the UAB Password/Passphrase Standard must be followed when changing such credentials.
2. Where possible, create standard user accounts for the operation of the IoT device/component. If possible, disable any default administrator account and create a custom administrator account. Be sure that the custom admin account is not named “admin” or “administrator.” Only use the admin account when such elevated privileges are required to make a change. Do not use an administrator account for standard operations.
3. IoT admins must actively identify such vulnerabilities and patch them as soon as possible. The availability of vendor patches also should be monitored on a regular basis.
4. Define the minimum services and features required to perform operations and enable just them. If a service or feature is not needed, disable it or, even better, uninstall it. Define a configuration guide that details the minimum required services and features and use follow that guide when building and configuring new IoT devices/components.
5. Vendors should provide a configuration guide. Follow the guide when building a device/component. Some vendors provide secure configuration (or “hardening”) guides. Ask the vendor about such guides and, if available, use them instead of standard configuration guides.
6. UPnP connections are not allowed or supported on the University’s network.
7. Create an initial inventory of IoT devices/components and their configuration specs. Maintain this inventory over time. When a new device/component is deployed, add it to the list. When an existing device is decommissioned, remove it from the list. When a device/component is patched, update its entry in the list. Review the list and audit the devices on a quarterly basis to ensure that the list is accurate. Address any gaps or issues discovered during the quarterly audit.
8. Where possible, avoid the use of MAC-based authentication in favor of a more robust authentication method. If MAC-based authentication is the only method of connecting to a wireless network, that device/component cannot be allowed to connect to any UAB network without being heavily segmented from UAB IT resources and traffic.
9. If the IoT device/component has PAN networking capability but that capability is not needed, disable the associated PAN wireless functionality.
10. Identify all data that will be transmitted/received by the IoT device/component in its IT environment. Maintain a record of the data types involved. Classify each data type following UAB’s [Data Classification Rule](http://www.uab.edu/it/home/component/k2/item/801-Data%20Classification%20Rule), and where necessary, protect Sensitive and Restricted/PHI data types using the controls mandated by UAB’s [Data Protection Rule](http://www.uab.edu/it/home/component/k2/item/818-data-protection-rule). Also, define and maintain a list of authorized protocols that are approved for use by the IoT device/component and in its associated environment. Ensure that only those authorized protocols are used and detect and eliminate any unauthorized protocols.
11. Network and host logs for the IoT device/component and its associated environment must be collected, stored, and reviewed on a regular basis. Reviews of the logs should focus on eliminating all instances of expected traffic and behavior so that anomalous activity can quickly be identified and investigated.
12. If the IoT device/component has WiFi SSID Broadcasting capability (2.4Ghz or 5Ghz), disable any feature that allows for broadcast of WiFi networks. This capability will cause interference with the campus WiFi air space. Any use of Campus WiFi spaces requires prior authorization.
13. If the IoT device/component utilizes Power-over-Ethernet (POE), VPIT reserves the right to remove any IoT device using excessive amounts of inline power. Campus network equipment has a limited amount of inline power available for use by IoT devices. If the power requirements exceed what is available, an external power injector may be required.
14. If the IoT device/components has the capability to act as an Ethernet hub or bridge, disable any unused interfaces
15. Many IoT devices go unmanaged once installed. These devices are prone to unpatched bugs and exploitation by hacking tools which may cause traffic patterns that affect campus core network. VPIT reserves the right to remove any IoT device from the campus network if the device is transmitting or receiving data that is harmful to the operation of the network.
16. Segmentation / Isolation

16.1 Cameras should be connected in collaboration with UAB Physical Security and provisioned into the Physical Security VLAN.

16.2 VOIP Phones and conference devices should be connected in collaboration with UAB Telecommunications and provisioned into the VOIP VLAN.

16.3 Access Control devices should be connected in collaboration with UAB Physical Security and provisioned into the Physical Security VLAN.

16.4 SCADA devices should be connected in collaboration with UAB Facilities and provisioned into the SCADA VLAN.

16.5 Network segmentation should be provisioned in accordance with the UAB’s [Data Classification Rule](http://www.uab.edu/it/home/component/k2/item/801-Data%20Classification%20Rule) and by UAB’s [Data Protection Rule](http://www.uab.edu/it/home/component/k2/item/818-data-protection-rule). If an IoT device processes or transfers Restricted data, if connected to the University network, it must be connected on a Restricted VLAN/Network.

16.6 General IOT devices that do not meet specific controls above should adhere to the [Acceptable Use Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000004.aspx).

#### **4.0 Enforcement and Implementation**

#### **4.1 Roles and Responsibilities**

Each University academic and business unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard security rule.

The Vice President of Information Technology Office is responsible for enforcing this standard security rule.

#### **4.2 Consequences and Sanctions**

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment. In the cases where students are involved, such issues will result in the reporting of a Student Code of Conduct violation.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the UAB network, disabled, etc., as appropriate until the device can comply with this standard.

#### **5.0 Exceptions**

Exceptions may be granted in cases where security risks have mitigating controls in place to lessen the intensity from a critical to a minimal level. To request a security exception, complete the [UAB Security Policy Exception](https://uabprod.service-now.com/service_portal?id=sc_category&sys_id=b179a61437d34e8024a67c1643990e80) Request from the UAB IT Tech Help portal.

1. **Definitions**
   1. **IOT (Internet of Things**): IoT consists of two foundational aspects—1) the Internet itself and, 2) semiautonomous devices (the “things”) that leverage inexpensive compute, networking, sensing, and actuation capabilities to sense the physical world and act on it. Such devices have the capability to connect to the Internet—being Internet Protocol (IP) based—but may also be deployed in stand-alone IP networks not connected to the Internet. These devices are unambiguously identified using the Web and Internet’s existing unique identification standards, such as the many Universal Resource Identifier (URI) schemes. With their sensor and activation capabilities, they establish relationships between the digital and physical worlds that did not previously exist. IoT includes the functions that allow users and organizations to analyze and understand the data gathered and actions taken by the things.
      * 1. An IOT device may be any physical object that conducts University business and may be connected to the Internet or campus network using wired or wireless technology. These devices have historically been stand alone or localized in communication, but now have extended modifications and technology allowing the device to communicate over the local network and Internet. Examples include (but are not limited to): cameras, temperature sensors, thermostats, desk phones, card readers, and lighting control systems. These devices typically do not allow user direct access to their underlying operating systems, management is generally direct-to-device (via html or console) or internet based (via a third party web site or smartphone application)
   2. **SCADA**: Supervisory control and data acquisition (SCADA) is a computer system used to monitor and control plant processes. As it relates to this policy, any IOT device used in conjunction with a SCADA system to provide sensor, monitoring, or operational functions.
   3. **User**: Any individual who performs University business.
   4. **User Account**: Information used by a user to gain access to UAB ePHI resources. This includes, but is not limited to, user IDs, passwords, personal identification numbers (PIN), tokens, certificates, biometrics, and smart cards.
   5. **User ID**: An individual ID used to identify a unique individual when logging into a UABHS information resource such as a computer network, service, or application
   6. **Camera:** any device used to capture and record still or motion images in any spectrum
   7. **VOIP (Voice over Internet Protocol) phones:** any device used to transmit voice communication data through the Universities central telecommunications infrastructure
   8. **Access Control devices**: Any device used to control access to University interior or exterior areas

**Change History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Description** | **Approval** | **Date** |
| 1.0 | Final version – approved by President Watts | Dr. Curt Carver | 9/20/2019 |
|  | Reviewed - no changes/updates |  | 2/12/2021 |
|  |  |  |  |
|  |  |  |  |