Internet of Things and Connected Devices Security For IT Leaders

This document is meant to be used as the basis for comprehensive policies, standards, and procedures around the use of connected devices within an organizational network. If you have a copy of this document, you are free to use any portion in part or in whole in your organization's internal documentation and IoT Security Plan. If you need assistance in implementing any component of this plan, please contact IoT Secure at info@iotsecure.io.

Last update: 2023

Powered by: IoT Secure™

Table of Contents

IoT Security and Your Organization

Whether you are a sole practitioner in your field and looking to ensure the security of your connected devices, or the CIO of a major enterprise with thousands of users and endpoints to manage knowing, assessing, and securing all connected devices is crucial to the continued security of the data and systems you protect. The below document was made to help you along in this journey by providing an outline of a policy along with explanations and descriptions to help you customize each section to better protect your connected devices.

As with any guidelines, regulatory requirements, or standards ever made, this alone will not secure your connected devices. It requires a complete device security program that is built from the ground up and enforced from the top down. Another part of this is the right tools, and IoT Secure designed the IoT Security Appliance (IoTSA) specifically with that purpose in mind. To learn more about our IoT security solution or to get your own FREE IoT-mini device to test on your network go here.

Sections One Through Three

The first four sections are intentionally designed to be generic enough to fit almost any organization. It is important to adjust these sections according to the specific goals, risk tolerance, and other variable factors related specifically to your organization. Otherwise, these first four sections, Objective, Scope, Background, and Definitions are just laying the groundwork for the document and are self-explanatory.

Objective

Our primary goal is to reduce risk associated with connected devices. The objective of this plan is to gather a comprehensive and accurate inventory of every connected device to our corporate network so we can identify and mitigate any vulnerabilities and risks.

Scope

This document establishes the minimum expectation to mitigate security risks common on connected devices, such as IoT, ICS, SCADA, and any other connected device that is not covered by other policies, like server, workstations, and laptops.

Definitions

IoT – Internet of Things is the overall category of connected devices that do not fit into traditional or common endpoints such as workstations, servers, laptops, etc.

Connected Devices – Connected devices include printers, multi-function devices, and basically any device that does not have a direct user interface, making it a slightly larger category than IoT.

Endpoint – Any device that connects to and communicates via a network, including all connected devices, computers, networking equipment, etc.

ICS – ICS, or Industrial Control Systems, are connected devices that control the automation of large-scale machinery. ICS can be anything from HVAC systems or fire suppression and alerting systems, to complex automated manufacturing lines.

SCADA – Supervisory Control and Data Acquisition is a control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level process supervisory management of connected control systems.

IT – Information Technology is the department or team typically responsible for the deployment and maintenance of network connected endpoints of all kinds.

IS – Information Security is the department or team responsible for information security. In smaller organizations, there may be overlap in the IT and IS teams.
Policy – Policy guidelines typically come from the highest levels of an organization, often approved and enforced at the CEO or Board level. Policies are meant to be relatively broad but should strive to ensure the overall safety and security of the organization.
Standards – Standards are one step down from the policy, and they typically are the responsibility of middle-management. Standards are updated less frequently than procedural documentation, but they should be reviewed and updated more regularly than the higher level policy documentation.
Procedure – Procedures are the lowest level of documentation in an organization. Procedures can vary between groups or even between employees in a group depending on the process they are describing. Procedures should match what is actually being accomplished each day in the real world and should be updated to reflect minor changes in workflow or processes.
Patching – Patching is the act of applying a software update to software. Patches are issued by official channels and should include comprehensive documentation on the changes the updates will make.
Vulnerability Scanning – Vulnerability Scanning is the act of using software to test endpoints connected to a network for potential vulnerabilities.
Monitoring – Monitoring is the continuous watching of a system's activity to identify any anomalies or unexpected changes in behavior so they can be investigated in a timely fashion.
Mitigation – Any act that fixes a risk or vulnerability in an endpoint.

Responsibilities

Section five is designed to clearly lay out the specific duties and responsibilities required to implement a competent connected device security. This section is significantly more maliable, and should be customized to match your organizations structure. For example, if you only have an IT department that handles IS functions as well, then they need to perform the IS duties laid out. Another example of a structure that would require change is in a common healthcare setup where many connected device and infrastructure are maintained by the "infrastructure" or "maintenance" teams. Finally, if any portion of the IT or IS for the organization is managed and supported by a third-party. In any of these cases, or your unique situation, the responsibilities can be assigned accordingly, but it is crucial that all of the responsibilities are handled by someone.

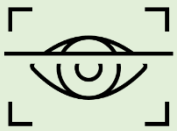
Responsibilities

Management/Supervision is responsible for ensuring that all corporate policy, standards, and procedures are in place, comprehensive, and above all, enforced. Management must maintain, update and ensure that approved guidelines are used and that documentation is updated appropriately. Without supervision, organizational policies, standards, and procedures can become a detriment to overall security.

Information Technology (IT) is responsible for maintaining a comprehensive and accurate inventory of every endpoint connected to the organizational network. IT must ensure that all identifying details of a device are added to the master inventory list before adding it to the network. As part of this process, IT works with respective departments to perform physical inventory checks and coordinate updates. Additionally, IT works with Information Security to assess and approve new devices, coordinate any notable inventory changes, and remediate or mitigate any vulnerabilities or risks.

Information Security (IS) is responsible for ensuring all devices and endpoints connected to the organization's internal network are secure. This process should include all endpoints that can connect to the intranet or internet via either a wired ethernet connection or a Wi-Fi connection. IS must perform a thorough security assessment of all connected devices to identify any risks and mitigate them before a device is deployed. This pre-deployment phase should be a joint effort between IT, IS, and the department in possession of the devices to ensure all parties understand the risks and use cases. The IS team should perform regular scanning and testing:

Basic discovery scans to ensure no new devices are online or that no devices have dropped off the network or changed IP (monthly).



Comprehensive vulnerability testing to include full-network vulnerability scans that use authentication when possible (quarterly).

Penetration testing to ensure any new vulnerabilities missed by the scanners are addressed (yearly).

Department in possession and/or uses the device is responsible for ensuring the devices are in a physically secure location. The respective departments also are responsible for performing regular physical inventory checks to ensure all devices are where they should be. The departments also must help schedule down-time for patching and scanning activities with the IT and IS departments.
All Employees are responsible for knowing this policy, ensuring that no unknown devices are connected to the network, and to go through proper channels when requesting or acquiring any new connected devices.

Training and Education

The sixth section of this template outlines the baseline education that all employees, as well as the various stakeholders should have in order to properly maintain the security and integrity of the data and devices in use. Like the previous section, it is important to customize this to best meet the unique circumstances at your organization. Like the responsibilities above, all of these are important to have covered by some stakeholders in the organization. So, like most of this document, those responsible for various aspects can be customized, but by no means should anything be cut and where applicable additional controls and measure should be added.

Training

All Employees – Some portion of the annual security awareness training should cover IoT and connected devices, including common misconceptions, risks, and procedures required to add or acquire new endpoints for the network.

Employees in the Departments in Possession of the device – IT and IS should provide a short presentation or video describing their responsibilities and liabilities in possessing any endpoints. This presentation or video should cover their responsibility to maintain the devices' physical security, usually by ensuring it is stored in a secure location or manner. The inventory and update/testing plan should be explained as well.

IT and IS Departments – At least one subject matter expert in each department should spend time and effort fully understanding any new device to be introduced to the internal network. This should include reading and understanding the manual, any APIs, and any other details available as well as a physical and logical inspection of the device to understand services, connections, ports, and other important details and settings.

Systems Criteria

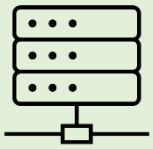
The last two sections are by far the densest and will probably be the most daunting to undertake. However, once you start to read through these sections it will quickly become clear that most of this is common sense (at least to a security or IT professional). This section must be customized to match with any policies, procedures or any applicable regulatory body your organization already follows.

Primary IoT and Connected Device Security and Systems Criteria

This policy document covers any device that connects to the network via ethernet (cat-5 or cat-6 connection) or via wireless network access (Wi-Fi). This plan is not intended to include "traditionally" managed devices like server, workstations, etc. that are managed via network policy and monitored through common means, such as SIEM or security management.

It is important to understand and acknowledge that ANY device that has an IP address and a MAC address is considered an endpoint and therefore requires administration, management, and security mitigation.

Pre-Deployment - Any devices fitting this criteria must be tested and authorized by the information technology and/or security group prior to deployment. This approval is required to prevent default configuration and password vulnerabilities. This testing should include checking for, at a minimum, the following common configuration issues:

	**Ensure the password is changed to a unique and complex password that meets the organizational password standards and is not reused on other devices.**
	**Test for unnecessary services such as FTP, unsecured web-based configuration pages, telnet, DNS, or any other active services that are not strictly necessary for the proper functioning of the device.**
	**If there is an HTTP or HTTPS based web configuration page, ensure it is not vulnerable. If it uses HTTP, disabled it and SSL/TLS should be tested to ensure it is not using a vulnerable version of SSL/TLS.**
	**Test the devices external connections (to the internet) to ensure they are strictly necessary to the functionality of the device. If any connected are not documented or appear to be collecting telemetry data, then those connections should be blocked by perimeter networking equipment if those connection cannot be disabled in the administrative setting of the device.**

Active Use - While in active use, the devices must be monitored for anomalies, regularly tested for new vulnerabilities, and patched when updates become available. IT, IS, and the department that possesses

the device should work together to regularly perform inventory, monitoring, scanning, and patching of these systems regularly and in a timely manner. The duties should be divided as outlined below:

Inventories are a joint task between the information technology team and the team or department that has possession of the device itself. Initially, before a device is officially deployed all unique details should be added to the overall asset inventory, this should be completed by the IT department. Beyond this the department in possession of the device will physically inventory and check the condition of the device on a regular basis. Suggested to do this as frequently as monthly and at least twice a year.

Inventory Responsibilities	
Information Technology	Maintain all endpoints in overall asset inventory.
Department in Possession	Physically check device details on regular basis and report to IT

Monitoring of Devices for anomalies, flaws, and new vulnerabilities is the responsibility of the information security (IS) team. Their responsibilities include active monitoring of any connected device with the overall organizational SIEM or via the SOC/NOC.

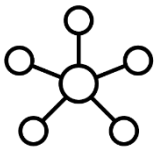
Regular Vulnerability Assessments should be conducted by the IS team to identify any new threats or vulnerabilities. These vulnerability assessments should be conducted at the same frequency as the organizational procedures call for scans of other endpoints. At a minimum these devices should be actively tested for new threats monthly.

Patching will need to be a task that requires input from IT, IS, and the department with possession of the device itself. Information Security will inform IT when a new patch is available or needs to be applied to a device or multiple devices. IT will test the patch on a device that is not currently in use to ensure it does not cause any issues. Once the patch is verified as safe to deploy the department that uses that device will need to coordinate with IT to schedule down-time in order to patch all affected devices.

Patching Responsibilities	
Information Technology	Test patch in safe manner. Coordinate with DIP for patch window.
Information Security	Inform IT when new patches are ready.
Department In Possession	Schedule down-time with IT to install patches on devices in department,

Secondary IoT and Connected Device Security and Systems Criteria

Alternative Mitigation Strategies

	**When it is not possible to patch a device, whether that patch is not available from the manufacturer or the patch is likely to break some critical functionality, then some of the below alternatives may be used to mitigate risks.**
	**When a flaw is "hard coded" into a device's firmware and cannot be changed (e.g. hard-coded passwords, ports open, weak TLS/SSL implementation, etc) then some of the below should be considered to mitigate the risks to the affected devices.**
	**When a device is known to make suspicious or insecure internet connections that cannot be turned off in the settings, then alternative mitigation (network segmentation and blacklisting) can be used to mitigate risk to affected devices.**

Network Segmentation

IT should use network segmentation when devices have known flaws or risks that cannot be remediated via settings or administrative changes. The flaws or risks can be to the endpoints themselves or to the data they process. For these devices, IT should set up a virtual LAN (VLAN) network segment that is more restricted than the other network segments. This strategy can allow the use of insecure or flawed devices within the network without putting the endpoints, data, or the rest of the network at increased risk of malicious attack.

Blacklisting (Firewall Blocking)

If devices are making outbound or inbound connections to the internet that are not strictly allowed per organizational policy, then adding the offending URLs and IPs to the perimeter firewalls' blacklists can help to mitigate the risk these connections present. Like other mitigating strategies, these should be used only once all other potential fixes have been exhausted.

Conclusion

This document will help you in establishing a more secure connected device security program but is by no means meant to be the complete package. The above guidance only works if followed, and supported by all stakeholders. In addition, there needs to be backing policies, standards and procedures to go into technical details of each portion.

As part of a complete and effective IoT security solution, the above guidance can be supported strongly by the use of IoT Secure IoT-mini security device. For qualified individuals and organizations, we will send you a FREE IoT-mini so you can begin the process of discovering, inventorying, analyzing, and securing your connected devices.