Home Office Network Asset Inventory

In this activity, I created an inventory of network devices connected to a home office network. The goal was to classify assets based on their sensitivity and importance to ensure proper protection of sensitive information. Below is the completed asset inventory, along with a detailed explanation of the process.

Asset Inventory Spreadsheet

Asset	Network Access	Owner	Location	Notes	Sensitivity
Network Router	Continuous	ISP	On-premises	Dual-band (2.4 GHz and 5 GHz). All devices connect to the 5 GHz frequency.	Confidential
Desktop Computer	Occasional	Homeowner	On-premises	Contains private information, such as photos and business documents.	Restricted
Guest Smartphone	Occasional	Friend	On and Off-premises	Connects to the home network. No sensitive data stored.	Internal-only
Printer	Occasional	Homeowner	On-premises	Stores temporary print jobs. No sensitive data stored long-term.	Internal-only
External Hard Drive	Occasional	Homeowner	On-premises	Contains backups of sensitive business and personal data.	Confidential
Webcam	Continuous	Homeowner	On-premises	Used for virtual meetings. No sensitive data stored.	Internal-only

Process and Methodology

Step 1: Identify Assets

I identified three additional devices connected to the home network:

Printer

External Hard Drive

Webcam

Step 2: Document Characteristics

For each device, I documented the following characteristics:

Network Access: How often the device connects to the network.

Owner: The person responsible for the device.

Location: The physical location of the device in relation to the router.

Step 3: Evaluate Network Access

I added notes for each device by considering:

The type of information stored on the device.

How the device connects to the network.

The level of security applied by the owner.

Step 4: Classify Sensitivity

I classified each device based on the potential impact of a security compromise:

Confidential: Devices containing sensitive information (e.g., Network Router, External Hard Drive).

Restricted: Devices with private information (e.g., Desktop Computer).

Internal-only: Devices used for business operations but with limited sensitive data (e.g., Printer, Webcam, Guest Smartphone).

Key Insights

Confidential Assets: The Network Router and External Hard Drive were classified as confidential due to their role in managing network access and storing sensitive data, respectively.

Restricted Assets: The Desktop Computer was classified as restricted because it contains private information, such as personal photos and business documents.

Internal-only Assets: Devices like the Printer, Webcam, and Guest Smartphone were classified as internal-only because they are used for business operations but do not store sensitive data long-term.

Why Asset Classification Matters

Classifying assets based on sensitivity is a critical step in asset management. It helps prioritize security efforts, ensuring that the most critical assets receive the highest level of protection. This approach minimizes the risk of data breaches, unauthorized access, and data loss while enabling efficient resource allocation and compliance with regulatory requirements.

Next Steps

This activity demonstrates my ability to:

- Identify and inventory network assets.

- Evaluate the sensitivity of assets based on their role and data stored.

- Apply appropriate security classifications to protect sensitive information.

This template and methodology can be adapted for professional use in asset management and cybersecurity projects. I have saved a blank copy of the template for future use in my portfolio and professional work.