# Smart Home Security

This playbook provides a sequential guide to securing your smart home devices. It outlines the steps necessary to protect against unauthorized access and cyber threats.

## Step 1: **Inventory**

Create a detailed list of all smart home devices. Include their makes, models, connection types, and what networks they are on.

## Step 2: **Updates**

Ensure all devices are running the latest firmware and software updates. Regularly check for new updates as they often contain security patches.

## Step 3: **Passwords**

Change all default passwords to strong, unique ones. Avoid using easily guessable passwords and consider using a password manager.

## Step 4: **Networks**

Secure your Wi-Fi network with WPA3 encryption, a strong password, and consider setting up a separate network exclusively for your smart devices.

## Step 5: **Features**

Disable unnecessary features on your devices that may open up security vulnerabilities, such as remote access if not needed.

### Step 6: **Permissions**

Review and limit the permissions granted to your smart devices. Only allow them to access what is necessary for their function.

### Step 7: **Monitoring**

Set up monitoring to alert you of any suspicious activity on your smart home devices or networks.

### Step 8: **Incident Plan**

Prepare a response plan for potential security incidents. This should include steps to isolate devices, change passwords, and notify any necessary parties.

# General Notes

## Regular Audits

Periodically perform security audits of your smart home setup to ensure compliance with the best practices and to identify any potential new vulnerabilities.

## Education

Stay informed about potential security threats to smart home devices and educate anyone else who has access to your smart home system about maintaining security.