
# Endpoint Security Policy

Last Review: January 2021
Next Review: June 2021
Effective Date: January 1st, 2021

Presented by:

## Tech Americas USA

# Contents

## Purpose

The purpose of this policy is to regulate protection of the customer network when accessed by Endpoint equipment such as laptops, tablets, and mobile devices. It is designed to protect our employees, customers and other partners from harm caused by the misuse of IT systems and data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

## Definitions

"Users" are everyone who has access to any of the Customer IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

"Systems" means all IT equipment that connects to a corporate network or accesses corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

## Objective

The objective is to reduce the risk of security breaches that could result from the connection and use of Endpoint devices. This policy seeks to limit security threats by:

- Ensuring Users are aware of the requirements and restrictions around Endpoint devices.
- Enabling protective measures and controls to manage Endpoint security and software compliance risks.

## Audience

Everyone who works at Tech Americas USA or anyone performing work on behalf of Tech Americas USA including contractors, consultants and volunteers are subject to this policy and responsible for the security of customer IT systems and the data on them. As such, everyone must ensure they adhere to the guidelines in this policy at all times.

## Scope

This policy covers all Endpoint devices connected to any customer network.

## Policy

This Audience is responsible for ensuring that:

## Information Security

- All care is taken to prevent unintended exposure, modification, or removal of private, copyright, or confidential information as a result of leaving this information on the screen or desk, or exposed in such a way that it can be viewed or accessed by an unauthorized individual. This includes information stored on portable storage media or hard copy.
- Any private, sensitive, or confidential information that is stored on such an Endpoint device has the appropriate security controls to restrict and prevent retrieval or intercept by an unauthorized third-party.

## End Point Software

All software contains security vulnerabilities, and software vendors are constantly supplying updates (patches) to address these vulnerabilities when they are identified.

- Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical to do so, i.e.:
    - Critical security patches are applied within 1 week of them being released by vendors
    - Important security patches are applied within 2 weeks of them being released by vendors.
    - Endpoint systems must be restarted following installation, to ensure security patches have been fully installed.
    - Where possible, it is recommended that Endpoint devices are set to auto-update their security patch levels, and restart if necessary to complete the installation.

## Computer and Data Security

If data on the Customer systems is classified as confidential users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Customer system any information that is designated as confidential, or that they should reasonably regard as being confidential to the Customer except where explicitly authorized to do so in the performance of their regular duties.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices.

Multiple layers of security practices should be utilized for devices connected to the Customer systems. These layers include firewalls, up-to-date anti-virus software, current software security patches and spyware removal and detection software.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the Customer systems by whatever means.

All devices being connected to Customer systems should be for professional use and not contain personal documents or any have any content related to activities that are inappropriate for the Customer to be associated with and/or are detrimental to the company's reputation, including pornography, gambling, inciting hate, bullying and harassment.

## Enforcement

Tech Americas USA will not tolerate any misuse of customer systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, Users should be aware that consequences may include the termination of their employment.

Use of any of the customer resources for any illegal activity will usually be grounds for summary dismissal, and Tech Americas will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

## Acceptance and Authorization

Performing service work by accepting a work order from Tech Americas USA implies acceptance of this policy. I have read and understand and agree to abide by its terms and conditions. I understand that violation of the use and provisions stated in the policy may result in limitations, suspension or dismissal, and/or disciplinary actions by Tech Americas USA or by legal authorities.


# Lounge Training TV Installation and BCM Phone System

# Contents

# Lounge Training TV & Cabling

## Overview

TJX (Marshall's, Homegoods, Home Sense & TJ Maxx) is installing a Training TV in the employee Lounge. The TV will be mounted on a rolling stand. One (1) cable will need to be run from the nearest MDF/IDF closet with an available switch ports between 41-46.
Training TV Cable will be terminated at the patch panel and RJ45 jack in a Cut-in plate 44" from floor near existing Time Clocks.

## Materials

TJX will ship the following materials direct to technician

- Stainless plate
- Purple RJ45 Jack (Training TV)
- Purple Patch Cord
- CAT5e Cable (Training TV)
- Technician will need to provide label printer and low voltage (cut-in) ring

## Assumptions

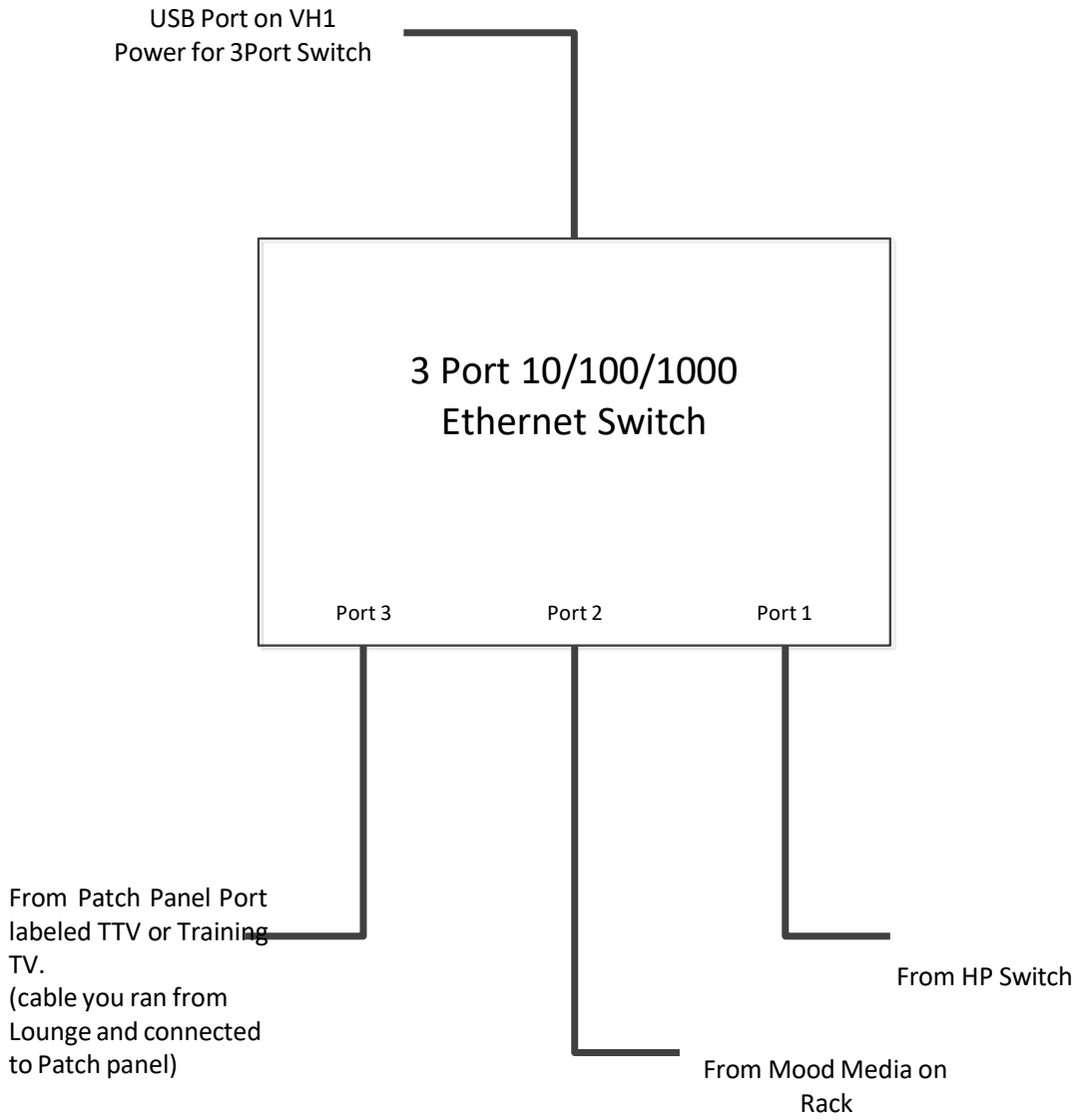
- Cable run should not exceed 300-feet. If run exceeds call TA PM/PC team at 281-668-3211
- Ceiling heights should not exceed 10 to 12-feet where the use of an 8 to 10-foot ladder could be used. If a lift is needed call TA PM/PC team
- Onsite environment assumes drop ceiling. If site ceilings are not drop ceiling call TA PM/PC team
- Equipment should not be damaged. If any of the equipment is found to be damaged or is missing anything, escalate to the TA PM/PC. Will need to also take pictures of damaged equipment and the box it was shipped in.

## Training TV and AP Cable Installation

1. Contact Tech Americas Call Center 281-668-3211 for Check-In and Security Code
2. Check-in on-site with Manager on Duty
3. Contact TJX Command Center to Check-In
    a. TJX Command Center 888.444.4848
    b. Option 1 English/Option 9/Option 5
    c. Option 9 and 5 are Silent Options. Wait for prompts
4. Locate Nearest Switch to Lounge with Port 41-46 available
    a. Only Switches are labeled H/H2/H3 can be used
        i. Labels on side of switch
        ii. Loss Prevention (LP) Switches H4/H5 not available
    b. IDF (ASM/Cash Office) – 41-46 Commonly Available
    c. MDF (System Room) – Only available if 2 or more switches installed
    d. MDF (System Room) If port 41 – 46 is not available you can share the line with the Mood Media player that is installed for the stores music using the 3 port switch you received.
        i. Connect the USB cable to VH1 server (used for power to the 3-port switch)
        ii. Disconnect the data cable from the existing Mood Media player located on the rack & connect it to port 1 on the 3 port switch. The other end connects to HP switch. Do not disconnect this cable from the switch.
        iii. Install a patch cord from port 2 on the 3 port switch to the existing Mood Media

player located on the rack.

iv. Install a patch cord from port 3 on the 3 port switch to the port on the patch panel labeled TTV or Training TV (new cable you installed).




5. Run 1 Cables from Nearest Patch Panel with Switch Port Available Port 41-26
    a. Training TV – Cut-in Plate 44" from floor near Time Clock
        i. Terminate RJ-45, install Stainless Wall Plate Label Training TV
            1. Remove protective coating from plate
        **ii.** Terminate at Panel, Test Cable & Label TTV or Training TV
6. Assemble Stand and Mount TV
    a. Mood Player Velcro Center Back of Stand
    b. TV Remote Velcro Back Left Stand
    **c.** Mood Remote Tether to Front Left Corner of Shelf
    d. Tether Mood Remote to Battery Door (Lower Half of Remote)
7. Connect Mood Player & Label Connections
    a. Label TV Power

b. Label Data

c. Label Plate

8. Contact TJX Command Center to Verify Player is On-Line
    a. TJX Command Center 888.444.4848
    b. Option 1 English/Option 9/Option 5
    c. Option 9 and 5 are Silent Options. Wait for prompts
    d. Verify Player Online
    e. Provide Return Shipping Number
        i. Label is shipped with Equipment
        ii. Return any 3-port switch, power adapter and all left over equipment
        iii. Leave with Manager
    f. Check out with the Command Center. If the site is complete, they will provide a SOT#. If the site is not complete, they will provide a TTR#, both which need to be recorded and provided to TA when checking out.

Documentation: All pictures will need to have a sticky note with the store # you are at, date, & name of technician.

    g. Picture of TV Back
    h. Picture of TV Front
    i. Picture of Wall Plate Labeled Training TV
    j. Picture of Patch Panel Labeled TTV or Training TV
    k. Picture of Switch Port used (ports 41-46).
    l. Picture of Return Shipping Label
    m. Picture of Completed Check-off List (attached)
9. Contact Tech Americas Call Center 281-668-3211 for Check-Out and Security Code
    a. Record SOT Number or TTR Number
    b. Verify all pictures uploaded (7-8 Pics)
    c. Fill-out attached Check-off list, take a photo of it and send it in with the other required photos to: documents@tech-americas.com

## Return Shipping

All Unused equipment must be boxed up by the technician re-using a box that was shipped to site & addressed to the following address to be shipped by the Store Management:

**Shipping Address:** Whalley Computer Associates
One Whalley Way
Southwick, MA 01077
Attn: TJX Depot (413) 569-420

# Appendix "B" – BCM Telephone System

1. The BCM Telephone System may be found on the shelf of the system rack inside the system room or on a wall located in the storage area or electric room inside the store. Confirm with the CC if the store has a BCM Telephone System.

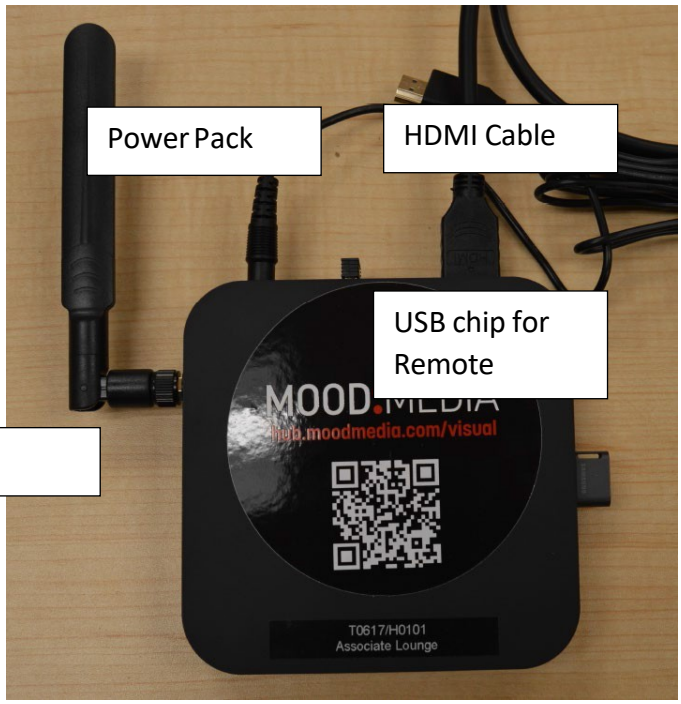
BCM

2. Disconnect the patch cable that connects to port 1 on the back of the BCM. The other end of the patch cable should connect to one of the ports 20-24 on the HP Network switch. Be sure to trace the cable back to the correct port and disconnect.
3. Once the patch cable is disconnected, call the Command Center and make sure that the CC is unable to see the BCM Telephone System (last octal will be .188 of the IP address).

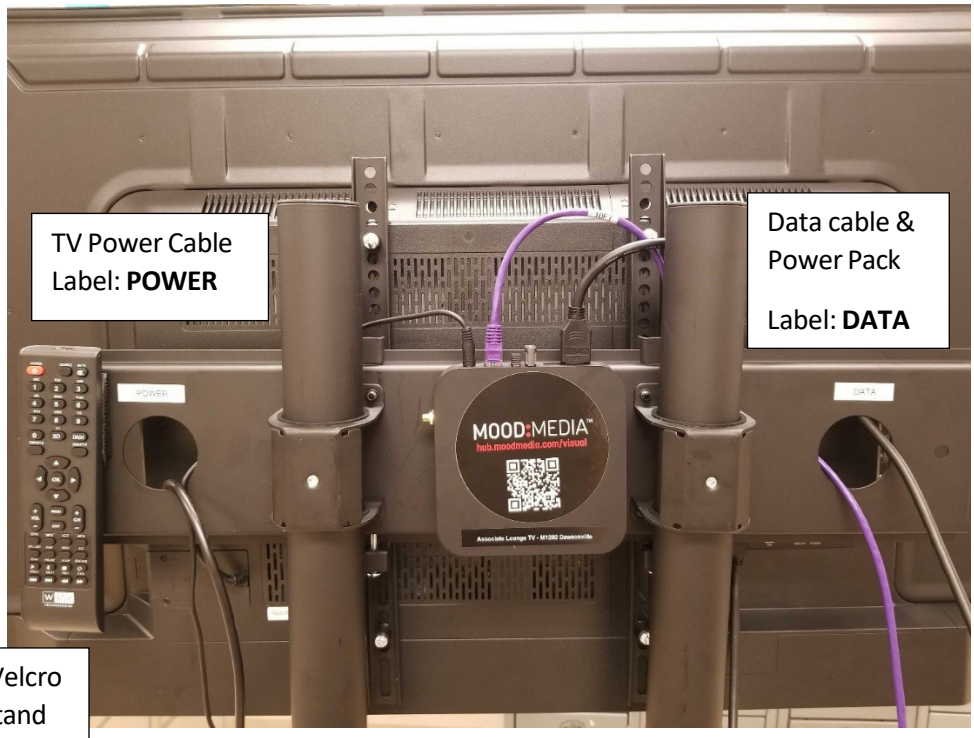
Figure A: Showing the BCM on System Rack
Disconnect from port 1 (second from left)

# Example Installation Pictures

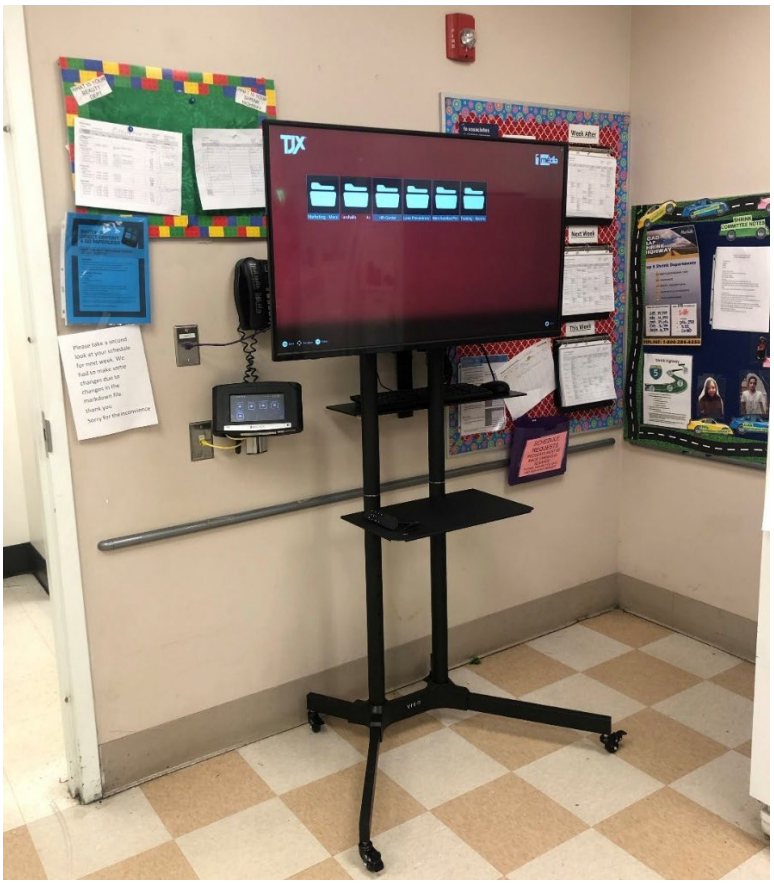
## Mood Media Equipment




## TV installation Back

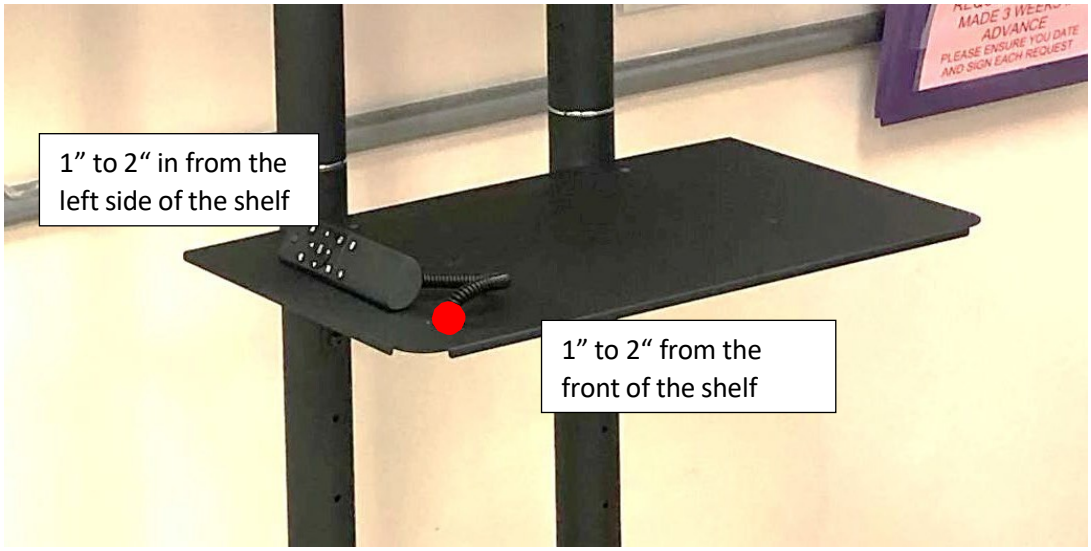


## TV installation Front



## Training TV Wall Plate Labeled Training TV (44” From Floor)

## Remote Tether Front Left Shelf (TETHER TO BATTERY DOOR BOTTOM HALF OF REMOTE)




## Patch Panel Labeled Training TV (TTV)/Lounge AP (LAP)

# Mood Media Checkout Sheet

Store Name:_____Store #:_____City:_____State:___

☐ Completed TV Stand Assembly

☐ Mounted TV to the TV Stand

☐ Mounted the Mood Media unit to the back of the TV Stand per procedures

☐ Attach the Mood Media remote to the TV Stand shelf as shown in the procedures

☐ Installed a new Cat5 cable from the Lounge Time Clock to the IDF patch panel

☐ Verified with the TJX Command Center that the Mood Media in the Lounge is online

☐ Verify with the TJX Command Center that the BCM is offline

☐ Store Management verified Installation was complete

☐ Took the following photos of the completed project: All pictures must have sticky note attached with the store # you are at, date, & name of technician.

- Front view of the completed Training TV
- Rear view of the completed Training TV
- Data jack for the Training TV
- Switch Port Connection (any available port 41 thru 46 only)
- Patch Panel labeled
- Return shipping label for unused equipment

Document any issues: _____

_____

_____

_____

Store Management Name: _____

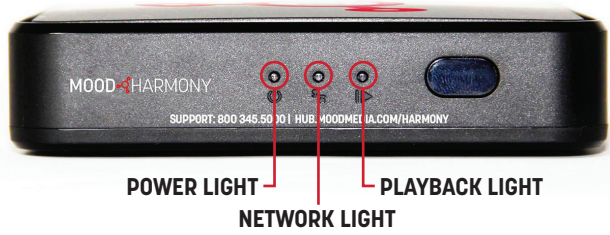
Store Management Signature: _____

# LED CONTROL GUIDE

Version 1.0

Your Mood Harmony device has 3 front-facing LED lights that provide helpful information. Use this guide to understand what the lights mean.

***NOTE:** Check **hub.moodmedia.com/harmony** for the latest version of this document.*




## POWER LIGHT

| LIGHT STATUS | MEANING | RESOLUTION |
|---|---|---|
| **Off** | No Power to the Device | Check that the device is plugged in to a working power outlet |
| **Solid Green** | Device is Powered On` | |
| **Solid Red** | Device is Asleep | Use the remote control to turn device on or power cycle the device |
| **Green / Red Slow** | Device is booting up - can take up to 2 minutes | If continues for more than 2 minutes, power cycle the device |
| **Green / Red Fast** | Receiving commands from the remote control | |

## NETWORK LIGHT

| LIGHT STATUS | MEANING | RESOLUTION |
|---|---|---|
| **Off** | No network connection | Check network cable and WiFi settings |
| **Solid Green** | Device connected to the Internet and communicating with Mood services | |
| **Solid Orange** | Device connected to the Internet but **not** communicating with Mood services | Contact your network administrator |
| **Green / Orange Slow** | Device is in hotspot mode. Setup using the Harmony Setup App on your mobile device. | Hotspot stays active for 10 minutes |
| **Green / Orange Fast** | Device is connected to the network but not connecting to the Internet | Contact your network administrator |
| **Orange Slow Blink** | WiFi not connected to the network | Use the Harmony Setup Mobile App to connect the player to the network |

## PLAYBACK LIGHT

| LIGHT STATUS | MEANING | RESOLUTION |
|---|---|---|
| **Solid Green** | Music is playing | |
| **Solid Red** | Playback hasn't started | Power cycle the media player if playback doesn't start after 2 minutes |
| **Green / Orange Fast** | Volume is muted or player is scheduled to be silent | Use the remote control to change volume or program |
| **Red / Orange Fast** | External storage (micro SD) is unplugged or damaged | Check / replace micro SD |