

# Audio-Video Conferencing Security Standard

## 1. Purpose

---

The purpose of this *AV Conferencing Security Standard* is to provide OUHSC personnel with notice of the minimum security requirements that must be in place in order to install and configure an AV Conferencing product suite.

## 2. Standard

---

- The Requestor's designated IS Administrator/user responsible for the device configurations are responsible for the following on a per deployment basis.
  - The requesting department will be responsible for providing the following information for each deployment for input onto the master campus resource lists.
  - Each Polycom endpoint deployment processed with Academic Technology (AT) for provisioning to the Video Infrastructure, will NOT need to go through a product review.
  - OUHSC AT will require the following, but not limited to:
    - IS Owner
    - IS Sponsor
    - IS Administrator
    - Location (Building, Rm number)
    - IP addresses and Host names for each device deployed.
- All systems should be located within the OUHSC Corporate Video Firewall.
  - Polycom RealPresence Access Director (RPAD) or Video Border Proxy (VBP) for H.323 and SIP signaling and media streams. These functions protect the open ports from internet-based attackers.
    - RPAD and VBP rules should be enabled and fine-tuned for each installation to block unwanted connections.
      - Dial rules to block known toll numbers or country codes that are not needed.
      - Guest dialing disabled to block calls coming from unwanted endpoints.
- The IS Administrator will ensure all Polycom codecs are registered by the Polycom Distributed Media Application Gatekeeper.
- The IS Administrator will ensure each device's user account be changed away from the default user account.
  - Passwords must meet OUHSC Password Policy.
- Remote management needs to be locked to internal IP addresses only.
  - Disable Web Management from external IP addresses. Disable if not in use.
  - Disable Telnet from external IP addresses. Disable if not in use.
  - Disable SNMP to and from external IP addresses. Update the default Community String from "public". Disable if not in use.
  - HTTPS should be forced on all management interfaces
- An active service contract must be maintained for each Polycom device to ensure all security patches and updates are available for each device.
- All Polycom UC devices need to be scanned for vulnerabilities every month. The IT Administrator is responsible to ensure each device follows the Vulnerability and Patch Management Policy and Standard.
- Auto Answer

- Disable if not in use
- If Auto Answer is enabled and in use.
  - Ensure “Mute Auto Answer Calls” is set as the College/Department requests. If no specific request is made, this feature should be set to “Mute Auto Answer Calls” by default.
  - Enable/Disable far end camera control is set as the College/Department requests. If no specific request, this feature should be Disabled by default.
  - Force camera lens cover, or camera to turn off when the system is not in use
- IS Administrator must monitor logs to ensure calls do not come in at unexpected/unscheduled times monthly
- All Video meetings should force encryption (AES) to prevent eavesdropping.
- When the Polycom UC reaches the end of life, the unit must undergo a Factory Reset, which restores the configuration to the initial, out-of-box configuration. This wipes all sensitive data (custom configurations, address book, call history, CDR logs, etc.).

### **3. Devices**

---

#### **A. VIDEOCONFERENCING CODEC**

Polycom: HDX codecs, Group Series codecs, Debut systems, Pano

#### **B. ROOM AUTOMATION**

Crestron: 3 Series, DM series, HD series, CCS series, AirMedia, TSW series, TS series, AMP series, GLS series, CEN series, C2N series

#### **C. PRIVATE NETWORK AVB SWITCH**

ExtremeNetworks: Summit series

Motu:AVB Switch

Netgear: ProSafe series

#### **D. WIRELESS PRESENTATION DEVICES**

Barco: CS series

WePresent

Crestron:AM series

#### **E. ROOM AUDIO MANAGEMENT**

Biamp – Tesira Series, Nexia Series, Avia Series

Crestron Audio –DSP Series

#### **F. LECTURE CAPTURE DEVICES**

Crestron CaptureHD

Mediasite Recorders - RL Series, ML900

#### **G. Displays and Projectors**

Panasonic: PT series

LG: LV Series, SM series

Sharp: PN & LC series

Samsung: D, E, F serie

#### **H. Blu-ray Players**

Samsung: BD Series

### **4. Related Documents**

---

- NIST Cybersecurity Framework (ID.RA, PR.DS, PR.IP, PR.PT)

- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(A)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(8)
- HIPAA Security Rule 45 C.F.R. § 164.310(a)(1)
- HIPAA Security Rule 45 C.F.R. § 164.312(a)(1)
- HIPAA Security Rule 45 C.F.R. § 164.316(b)(2)(iii)
- HIPAA Security Rule 45 C.F.R. § 164.308(b)(1)
- HIPAA Security Rule 45 C.F.R. § 164.308(b)(2)
- HIPAA Security Rule 45 C.F.R. § 164.312(e)(1)
- HIPAA Security Rule 45 C.F.R. § 164.312(e)(2)(i)
- HIPAA Security Rule 45 C.F.R. § 164.312(e)(2)(ii)
- HIPAA Security Rule 45 C.F.R. § 164.314(b)(2)(i)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(i)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(D)
- HIPAA Security Rule 45 C.F.R. § 164.312(b)
- HIPAA Security Rule 45 C.F.R. § 164.312(e)
- Payment Card Industries Data Security Standard (PCI DSS) version 3.2

## 5. Scope

This Standard is applicable to all OUHSC faculty and staff who may configure an **Audio-Video Conferencing product suite**<sup>[BLD(1)]</sup>.

## 6. Revision, Approval and Review

### 6.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	02/13/2017	Campus IT	Baseline Version
1.1	03/08/2017	Campus IT	Added a requirement
1.2	09/18/17	IT Security	Product Review is no longer required when AV systems are ordered/processed through AT

### 6.2 Approval History

Version	Date	Approved By
1.0	02/14/2017	
1.1	03/09/2017	