UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Standard

Audio-Video (AV) and Conferencing Tools Security Standards

Current Version	Compliance Date	Approved Date
1.4		

1. Purpose

- The purpose of this *AV & Conferencing Tools Security Standard* is to provide OUHSC personnel with notice of the minimum security requirements that must be met in order to install and configure approved AV or Conferencing products on the OUHSC IT network.
- An *OUHSC Information Security Risk Assessment (Product Review)* has been completed for all equipment listed in **Sections 3 and 4**. If your device(s) is not listed in Section 3, you must initiate a Security Risk Assessment for said device(s). Start the process here: https://it.ouhsc.edu/forms/productreview.asp

2. Polycom (Poly) Videoconferencing Codec Deployment Standards

Section 2 applies to the deployment of Polycom (Poly) videoconferencing devices onto the HSC Video Infrastructure and IT Network. All **IS Administrators** are required to adhere to the following standards.

A. Polycom (Poly) codecs sold and deployed through Academic Media & Digital Services or Academic Technology (AT) will **NOT** need to undergo a product review, see **Section 3: Approved Polycom (Poly) Devices**.

B. All Polycom (Poly) codecs placed on the OUHSC IT Network MUST be provisioned and joined to the campus Polycom Video Infrastructure, find more information here: https://www.ouhsc.edu/at/Videoconferencing.aspx.

C. All Polycom (Poly) codecs will reside behind the *Polycom RealPresence Access Director (RPAD)* also known as the OUHSC Video Firewall Traversal. The RPAD appliance enables users within and beyond the firewall, to securely access video services-whether at home, in the office or on the go. It securely routes communications, management and content through firewalls without requiring additional client hardware or software.

D. All Polycom (Poly) codecs will be provisioned by the *Polycom RealPresence Resource Manager (RPRM)*. The RPRM appliance provisions, manages and monitors hundreds of video devices across a global network. Through the customizable dashboard for each administrative user, you can manage and troubleshoot all Polycom video devices.

E. All Polycom (Poly) codecs will be registered to the *Polycom Distributed Media Application gatekeeper (DMA)*. The DMA is a network based appliance that manages & distributes calls across collaboration networks. The DMA dynamically routes calls throughout the network based on priority, class of service, resource availability, and network outage with highly efficient load balancing and virtualizing of bridging resources.

F. An active Polycom (Poly) Maintenance Contract must be renewed annually for each codec in order to remain in compliance. IT Security mandates all codecs deployed on the IT Network possess the latest software and security patches.

G. All Polycom (Poly) devices will be scanned for vulnerabilities every month. The **IS Administrators** are responsible for ensuring each codec follows the *Vulnerability and Patch Management Policy and Standard* found here: https://it.ouhsc.edu/policies/documents/infosecurity/Vulnerability%20Management%20Policy.pdf.

H. **IS Administrators** must monitor logs to ensure calls do not come in at unexpected/unscheduled times monthly.

3. Roles and Responsibilities

The **IS Administrator** *(user responsible for Polycom codec configuration)* will provide the following information to Academic Technology (AT) for each Polycom (Poly) deployment:

- IS Owner
- IS Sponsor
- IS Administrator
- Physical location of codec (Building, Room number)
- IP addresses and Host names for each codec.

The **IS Administrator** will verify the following configurations are applied to the codec:

- Ensure *"LAN Speed"* is set to *"100 Mbps"*.
- Ensure *"Duplex Mode:"* is set to *"Full"*.
- Ensure *"Dynamic Bandwidth:"* is NOT checked.
- *"Require AES Encryption for Calls:"* will be set to *"When Available"*.
- Change codec default *"Admin ID:"* ("Admin" account) password for GUI remote management access.
  - Passwords must meet OUHSC Password Policy: https://it.ouhsc.edu/policies/Password_Management_Policy.asp
- Ensure *"Enable Web Access:"* is checked.
- Ensure *"Restrict to HTTPS:"* is checked.
- Ensure *"Enable Telnet Access:"* is NOT checked.
- Set *"Lock Admin Account After Failed Logins:"* to *"5"*.
- Set *"Admin Account Lock Duration:"* to *"5 minutes"*.
- Ensure *"Lock User Account After Failed Logins:"* is set to *"5"*.
- Ensure *"User Account Lock Duration:"* is set to *"10 minutes"*.
- Ensure *"Enable SNMP:"* is checked.
- Disable *"Auto Answer Point-to-Point Video:"* when possible.
  - If *"Auto Answer Point-to-Point Video:"* is enabled:
    - *"Audio mute auto answered calls:"* can be set as the College/Department requests; however, *"Audio mute auto answered calls:"* is checked, if no specific request is made.
    - *Enable/Disable "Allow Other Participants in a Call to Control Your Camera:"* as the College/Department requests. Disable by default, if no specific request is made.

3. Approved Polycom (Poly) Devices

IT & AT only endorse the following Polycom (Poly) videoconferencing devices:

- Polycom (Poly) Group Series codecs.

4. Approved Accompanying Audio-Video Devices

Section 4 applies to other Audio-Video devices that typically accompany a Polycom (Poly) codec in a standard videoconferencing equipped learning or collaborative space. The following approved devices can be deployed and installed on the OUHSC IT Network.

An *OUHSC Information Security Risk Assessment (Product Review)* has been completed for all equipment listed in **Sections 3 and 4**. If your device(s) is not listed in Section 3, you must initiate a Security Risk Assessment for said device(s). Start the process here: https://it.ouhsc.edu/forms/productreview.asp

A. ROOM AUTOMATION

- Crestron: 2, 3, & 4 Series, DM series, HD series, CCS series, AirMedia, TSW series, TS series, AMP series, GLS series, CEN series, C2N series.
- Atlona: AT – HDR, HDVS, JUNO, OME, OMIN, OPUS, UHD series

B. PRIVATE NETWORK AVB SWITCH for AV use only

- ExtremeNetworks: Summit series
- Motu: AVB Switch
- Netgear: ProSafe series
- Pakedge: S3 series

C. WIRELESS PRESENTATION DEVICES

- Barco: CS series WePresent
- Crestron: AM, Mercury series

D. ROOM AUDIO MANAGEMENT

- Biamp – Tesira Series, Nexia Series, Devio series
- Crestron – Avia series
- Vaddio – EasyUSB Series

E. LECTURE CAPTURE DEVICES

- Mediasite Recorders – RL 8XX, 9XX, 2XX, 3XX Series, ML 8XX, 9XX Series

F. DISPLAYS & PROJECTORS

- Panasonic: PT series
- Epson: PowerLite & Pro series
- LG: LV Series, SM series
- Sharp: PN, LC, UH series
- Samsung: B, D, Q series

G. BLU-RAY PLAYERS

- Samsung: BD Series

5. 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

6. Scope

This Standard is applicable to all OUHSC staff and faculty who may configure an Audio-Video Conferencing device.

7. Revision, Approval and Review

7.1 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
1.3	04/19/2018	IT Security	Added Mercury presentation device
1.4	04/13/2020	AT	Added Mediasite model versions

7.2 Approval History

Version	Date	Approved By
1.0	02/14/2017	
1.1	03/09/2017	
1.2	?	
1.3	?	
1.4		