1. Introduction

This document establishes the technology and audiovisual (AV) standards for the San Diego Community College District (SDCCD). These standards support modern teaching and learning environments, focusing on accessibility, hybrid learning capabilities, and secure network integration across district-wide systems.

The standards apply to classrooms, lecture halls, meeting rooms, and study spaces, ensuring consistency, functionality, security, and accessibility for students and faculty in compliance with California and federal accessibility and IT security laws, including ADA, Section 508 of the Rehabilitation Act, California Government Code 11135, and cybersecurity policies for network infrastructure.

2. Technology & AV Standards by Category

2.1 Projectors (Short Throw vs. Ceiling Mounted)

Short Throw Projectors (For Small and Medium Classrooms)

- Ultra-short throw (UST) laser projectors (minimum 4,000 lumens).
- Wall-mounted near the display surface.
- No need for pull-down screens in small rooms with a matte-finish wall.

Ceiling-Mounted Projectors (For Large Classrooms & Lecture Halls)

- Laser-based projectors (minimum 5,000 lumens).
- Mounted with secured brackets.
- Motorized pull-down or fixed screens.

Accessibility & Network Compliance:

- Must be connected to the district network for remote management and firmware updates.
- Secure wireless connectivity required for faculty and student device screen sharing.
- Must be configured to prevent unauthorized external connections to maintain cybersecurity standards.

2.2 Digital Displays

- 75-inch or larger 4K commercial-grade screens.
- Wall-mounted at an optimal viewing height for seated and standing users.
- Multi-touch and interactive capability for enhanced engagement.
- Text-to-speech and screen magnification options for accessibility.

Network Compliance:

- Must be configured to use the SDCCD Wi-Fi and VLAN segmentation for device security.
- Displays must support encrypted wireless and wired connections to prevent data interception.

2.3 Podiums & Lecterns

Technology (Computers, Switch Controllers)

- Podiums must be height-adjustable for standing or seated users.

- Integrated desktop computers with speech-to-text and screen-reader software.
- Switch controllers and touchscreens with high-contrast settings and voice-command capabilities.
- Secure district login required for podium computers.

Network Compliance:

- All podium computers must use district-approved authentication methods (Single Sign-On with Multi-Factor Authentication).
- Only district-approved software and networked applications are allowed on podium computers.

2.4 Microphones & Speakers

- Wireless lapel and handheld microphones.
- Ceiling or wall-mounted speakers for even sound distribution.
- Assistive listening devices (ALDs) such as hearing loop systems.
- Live captioning integration for hybrid learning platforms.

Network Compliance:

- Microphone systems must be integrated with SDCCD's AV network for centralized control.
- Wireless microphones must use secure frequencies to prevent interference or unauthorized access.

2.5 Cameras (For Hybrid & Lecture Capture)

- Pan-Tilt-Zoom (PTZ) cameras with auto-tracking.
- One front-facing camera for the instructor, additional cameras for student engagement.
- AI-powered auto-captioning for recorded and live-streamed lectures.
- Compatible with screen readers and text magnification software.

Network Compliance:

- Cameras must be connected to SDCCD's secure video management system.
- End-to-end encryption is required for video streams to prevent data leaks.
- Must support district-approved integration with Zoom, Microsoft Teams, and LMS platforms (Canvas).

2.6 Access Points for Wireless Services

- Wi-Fi 7E for high-density, low-latency connectivity.
- Evenly distributed ceiling-mounted access points.
- Accessible login portals for students using assistive devices.

Network Compliance:

- All classroom Wi-Fi access points must be part of SDCCD's managed network infrastructure.
- Separate VLANs for faculty, students, and guest access to ensure security.
- 802.1X authentication is required for faculty and district-managed devices.

2.7 Desktop Computers for Students

- Adjustable height desks to accommodate mobility devices.
- Pre-installed with:
  - Screen readers (e.g., NVDA, JAWS, Voiceover).
  - Speech-to-text software (e.g., Dragon NaturallySpeaking).
  - Color contrast and magnification options for low-vision users.

Network Compliance:

- District-approved security policies must be used, including firewall rules and endpoint protection.
- Only SDCCD-approved applications can be installed.
- Automated session logoff after inactivity to protect user privacy.

2.8 Emergency Call Appliances (Red Call Buttons)

- Wall-mounted at an ADA-compliant height for easy access.
- Near entry and exit doors, podiums, and designated ADA seating areas.
- Visual and audio alerts for individuals with hearing or vision impairments.

Network Compliance:

- Emergency call appliances must be integrated into SDCCD's VoIP and dispatch system.
- Dedicated VLAN and power backup to ensure emergency functionality during outages.

3. **Compliance with Network & Wi-Fi Standards**
All AV and technology components must adhere to SDCCD's IT security and network policies, including:

3.1 Secure Network Access

- All devices must authenticate to SDCCD's network using secure credentials.
- Devices must be assigned to the correct VLAN based on their role (faculty, student, guest, emergency).
- Unauthorized devices are prohibited from connecting to SDCCD's secure network.

3.2 Data Security & Compliance

- End-to-end encryption required for all AV streaming and data transmission.
- Regular security audits for connected devices to prevent vulnerabilities.
- Compliance with FERPA and CCPA for any recorded or transmitted classroom data.

3.3 IT Management & Support

- All AV devices must be centrally managed by SDCCD's IT department.
- Firmware updates and patches must be applied regularly to prevent security risks.
- IT staff must have remote monitoring and control capabilities to troubleshoot issues.

4. **Implementation & Maintenance**
- Routine Accessibility & Network Audits:

- Conducted each semester to test AV controls, emergency appliances, and network security.
- Software Updates:
- Quarterly updates for captioning software, network firmware, and security patches.
- Faculty & Staff Training:
- Annual workshops on secure technology use, network compliance, and ADA standards.

5. Conclusion

SDCCD's AV and technology standards provide a fully accessible, hybrid-ready, and secure learning environment for students and faculty. By adhering to ADA, Section 508, California accessibility laws, and SDCCD's network security policies, these standards ensure equitable access and data protection for all users.

These specifications will be reviewed and updated regularly to align with emerging educational technologies, network security best practices, and compliance requirements.