

Procedures And Policies Concerning The  
Use Of Louisiana Board of Regents  
Equipment While Conducting Distance  
Learning Classes With Video Conference  
Components

---



**Contents**

- Introduction ..... 1
- Security Policies ..... 2
- Equipment Maintenance and Network Connectivity ..... 3
- Schedule Maintenance For Classes And Class-Related Events ..... 4
- Endpoint Connectivity For Classes And Class-Related Events ..... 6
- Software Required For Execution Of Outlined Procedures ..... 9
- Removal or Modification of Scheduled or Running Conferences by BoR..... 10
- Appendix A: Firewall Information ..... 11



## Introduction

BoR<sup>1</sup> provides **access** to centralized equipment (belonging to BoR) for use by institutions wishing to schedule, conduct, and connect to distance learning classes with a video conferencing component. The primary purpose of this access is to provide a means for institutions to conduct said classes when the institution does not have the necessary resources onsite.

As distance learning classes are not the only video conferences conducted on BoR equipment, BoR must take care to ensure that both class and non-class events do not result in resource or scheduling conflicts on BoR equipment. To facilitate the management of BoR equipment and to help ensure the above, the procedures and policies outlined in this document have been put in place with the goals of:

- providing orderly and traceable user access to BoR equipment
- ensuring proper utilization of resources on BoR equipment
- avoiding conflicts between scheduled classes, unscheduled class events, non-class events, and scheduled maintenance on BoR equipment
- providing efficient management of class endpoint connectivity to BoR equipment

**While BoR will act in good faith to provide reliable up time of the BoR equipment as well as reliable access to the BoR equipment, nothing in this document implies a guarantee of any specific up time of the BoR equipment, access to the BoR equipment, or level of service from BoR.**

**This manual is solely maintained by BoR.**

---

<sup>1</sup> The term “BoR” is used throughout this document as an abbreviation for the Louisiana Board of Regents

## Security Policies

The information in this section describes security policies implemented by BoR to provide orderly and traceable user access to BoR equipment.

1. Any user of BoR equipment **MUST** have valid user credentials issued by BoR for use on BoR equipment.<sup>2</sup>
2. All users of BoR equipment are responsible for protecting their BoR equipment user credentials and will be considered responsible for any actions performed using their credentials.
3. All users of BoR equipment **MUST** ensure that, unless they have been given **EXPLICIT** permission by BoR to do so, they do not use their access privileges to:
  - Add, remove, or modify any settings or configurations on BoR equipment
  - Add, remove, or modify any user credentials on BoR equipment
4. A user's access level does not equate to BoR's **EXPLICIT** permission to perform any action.
5. Non-BoR users may not access BoR equipment except through BoR-approved means.
  - As of the writing of this document, the only BoR-approved means of access to the RMX is the Polycom RMX Manager software available via the BoR equipment.

**Failure of any participating institution or user to adhere to these security policies or to follow any procedure outlined in this document may result in suspension of or full revocation of permission to use BoR equipment for video conferencing during distance learning classes.**

**The procedures and policies outlined in this document are solely enforced by BoR.**

---

<sup>2</sup> While not recommended by BoR, participating institutions may "share" user names among multiple people at said institution. When this occurs, the user name will be considered one user and will be held responsible for any actions performed using the user name. This results in the entire group of people "sharing" the user name being held accountable for any actions performed using this user name.

## Equipment Maintenance and Network Connectivity

The information in this section describes the responsibilities of the various parties involved in maintaining the equipment and network connectivity necessary for the successful scheduling and conducting of video conferences for distance learning classes utilizing BoR equipment.

1. BoR is responsible for maintaining equipment belonging to BoR **ONLY**.
2. BoR is responsible for maintaining reliable network connectivity to the **inner edge**<sup>3</sup> of the BoR network for equipment belonging to BoR **ONLY**.
3. BoR is responsible for assuring it does not make any changes to settings or configuration on equipment not belonging to BoR without the **EXPLICIT** permission and input of the technical resources responsible for said equipment.
4. Each participating institution is responsible for maintaining equipment belonging to said institution **ONLY**.
5. Each participating institution is responsible for maintaining reliable network connectivity to the **outer edge** of the BoR network for equipment belonging to said institution **ONLY**.
6. Each participating institution is responsible for assuring it does not make any changes to settings or configuration on equipment not belonging to said institution without the **EXPLICIT** permission and input of the technical resources responsible for said equipment.

**A dedicated machine will be provided and maintained by BoR in BoR's equipment rack for use by technical resources at participating institutions. The purpose of this machine is strictly to provide a platform and tool suite (ping, traceroute, nuttcp for bandwidth test, etc.) to be used by technical resources at participating institutions while troubleshooting network connectivity issues between said institutions and BoR's networks. This machine will be connected directly to one port of the BoR edge switch; BoR equipment mentioned elsewhere in this document will be connected directly to different port(s) of this switch.**

**Access to this dedicated troubleshooting machine will be remote only via SSH and is solely controlled by BoR. Any users granted access to this machine will require a different set of user credentials than the ones mentioned in the Security Policies section of this document; however, the same security policies apply.**

**BoR EXPLICITLY FORBIDS any execution of bandwidth tests utilizing this dedicated troubleshooting machine without prior scheduling and written (email) approval from BoR.**

**BoR reserves the right to immediately terminate any testing which is determined to cause a stability or resource issue on BoR's equipment or network.**

---

<sup>3</sup> The switch housed in BoR's equipment rack is considered the edge of BoR's network (ip: 76.165.208.1).

## Schedule Maintenance For Classes And Class-Related Events

The information in this section describes the procedures as well as the responsibilities of the various parties involved in maintaining the schedule of video conferences for distance learning classes on BoR equipment.

1. BoR does not limit the scheduling of classes to BoR working days<sup>4</sup> or BoR working hours<sup>5</sup>.
2. Participating institutions **MUST** have a designated scheduling coordinator whose responsibility it is to make and maintain the schedule of classes on BoR equipment for any class conducted by the institution.
  - a. Scheduling coordinators have BoR's permission to modify the conference reservations on BoR equipment **only as they pertain to the schedule of classes.**
  - b. A participating institution may grant permission to manage its class schedule to a scheduling coordinator from another institution. BoR does not require notification of this agreement and the enforcement of the agreement falls solely on the institutions involved.
3. When maintaining the schedule of classes on BoR equipment, scheduling coordinators **MUST**:
  - a. Coordinate with and collect all relevant information including contact information for endpoint technical support from all institutions involved before scheduling or modifying a scheduled class
  - b. Create and maintain the conference reservations for scheduled classes on the BoR equipment
  - c. Ensure they only modify conference reservations for which they are directly responsible
  - d. Notify BoR in writing (email) when any of the following changes to the class schedule are made:
    - A class is first scheduled
    - A class reservation is modified
    - A class is cancelled (entire reservation or one instance)
  - e. Provide the following information to BoR in writing (email) before a class is added to the schedule:
    - Contact information for scheduling coordinator responsible for class, including BoR equipment user name
    - All participant endpoints for class
    - Designated instructor endpoint
    - Designated monitoring institution(s), including BoR equipment user name(s)
    - Days and times of class
    - Days and times of the conference reservation
  - f. Format the conference name for a scheduled class as schedulingInstitution\_monitorInstitution\_classTitle (ex. BOR\_BOR\_Scheduling101). This

---

<sup>4</sup> the term "BoR working days" is defined as Monday through Friday (excluding scheduled BoR holidays).

<sup>5</sup> the term "BoR working hours" is defined as 8:00 a.m. to 4:30 p.m. CT on BoR working days.



## Endpoint Connectivity For Classes And Class-Related Events

The information in this section describes the procedures for maintaining endpoint connectivity as well as the responsibilities of the various parties involved both before and while a scheduled class is being conducted.

1. A test session which connects all relevant endpoints to BoR equipment **SHOULD** be performed a minimum of five (5) BoR working days before the first meeting of a scheduled class. This test is to verify the required settings necessary to successfully connect each endpoint to BoR equipment.
  - a. The timing of this test must be coordinated with BoR and formally scheduled/performed during BoR working hours with BoR participation.
  - b. Someone should be present at each endpoint to verify the connection.
  - c. If, during this test, the auto-dial from BoR equipment cannot reach an endpoint configured as dial out, but the endpoint can dial into the BoR equipment, the endpoint must be configured as a dial in connection for the reservation. BoR is not responsible for providing technical support to determine why the dial out autodial does not connect to the endpoint.
  - d. If, during this test, a reliable connection cannot be established with an endpoint and the BoR equipment/network is determined to be functioning, it is the responsibility of the endpoint's technical resources to troubleshoot the issue before rescheduling a new test. If requested, BoR, may, at its discretion, **ASSIST** with troubleshooting before the new test.
  - e. **While this test is not required, if it is not performed or is not completed successfully, BoR will not provide assistance for any issues arising while this class is being conducted.**
2. The responsibility of monitoring classes or class-related events for the purpose of ensuring participant connectivity falls primarily to monitors designated at the time of scheduling.
  - a. Designated monitors have BoR's permission to:
    - maintain the participant endpoint list of a class conference running on BoR equipment (connect and disconnect participants)
    - modify the participant endpoint list of a class conference running on BoR equipment (add or remove participant endpoints)
    - end a class before its scheduled end time and remove it from the list of currently running conferences (this includes removing the conference reservation before the class starts)
  - b. In the event that a reliable connection for an endpoint cannot be made or held while a class or class-related event is being conducted, it is the designated monitor's responsibility to either restore connectivity or notify the endpoint's technical resources of the issue.
    - i. It is the responsibility of the endpoint's technical resources to verify the following:

- the endpoint equipment is in working order
  - there is a reliable route to and from the endpoint equipment to the outer edge of the BoR network
  - all necessary traffic is allowed to pass through any network devices under the control of the participating institution which are between the BoR equipment and the endpoint (e.g., firewall rules are in place to allow necessary traffic to and from the endpoint)
- ii. Only after assuring (i) above should the endpoint's technical resources contact BoR to request assistance with the issue.
1. The initial contact should be in writing (email) and should include the following information:
    - all relevant contact information for the technical resource responsible for this issue
    - class conference name
    - description of problem, including time of occurrence and remedies already attempted
  2. BoR will attempt to respond in a timely manner; however, there is no guaranteed response time. In the event the request is made after hours,<sup>6</sup> BoR, may, at its discretion, wait until BoR working hours to respond.
  3. BoR, may, at its discretion, decline this request for assistance. Examples of issues for which BoR may decline a request for assistance (not an exhaustive list):
    - the issue is recurring and has previously been traced to a problem with the specific endpoint
    - the issue has previously been traced and determined to be an issue with the institution's or an intermediary network
    - it is an obvious issue caused by configuration out of BoR's control (e.g., endpoint is not properly NATted)
- iii. Technical resources have BoR's permission to:
- create ad-hoc video conferences for the purposes of testing endpoint connectivity
  - modify the participant endpoint list of a class conference running on BoR equipment (add or remove participant endpoints)
- iv. The conference name of any ad-hoc testing conferences created by technical resources should be formatted as  
 test\_technicalResourceInstitution\_classTitle\_description (ex.  
 test\_BOR\_Scheduling101\_ConnectivityIssue).

---

<sup>6</sup> the term "after hours" is defined to mean any time outside of BoR working hours.

3. If an endpoint in a class or class-related event conference is configured as dial in, it is the participating institution's responsibility to have someone available, trained and willing to initiate and maintain the connection.
4. It is **recommended** that all dial out endpoints be fully powered on no less than 20 minutes before a class is scheduled to begin. This will alleviate the issue of endpoints not connecting due to missing the BoR equipment's auto dial 15 minutes before the start of class.
5. It is **recommended** that all dial in endpoints dial the BoR equipment at 10 minutes before the start of class. This will alleviate the issue of endpoints attempting to connect before the conference has been started in the BoR equipment, while still providing a "buffer" to handle any last-minute issues.
6. BoR, may, at its discretion, monitor scheduled classes via software or video participation for the purpose of maintaining BoR equipment and/or network connectivity.

**The connectivity of a direct-dialed connection is the responsibility of the participating institutions involved and any issues arising from said connection should be handled by the participating institutions.**

## Software Required For Execution Of Outlined Procedures

This section provides notification to participating institutions that BoR will provide **ACCESS** to software required to execute the procedures outlined in this document.

1. Persons delegated with the tasks outlined elsewhere in this document will be provided access to software required to perform their respective responsibilities
2. BoR, when required, may provide basic training on specific tasks necessary for execution of the procedures outlined in this document
3. BoR makes no guarantee that said software will function correctly at every site and will not provide support for any technical issues arising during the installation, maintenance or execution of the required software
4. In the event the required software will not function correctly at a specific site, BoR will provide access to the software via an industry standard remote connection to a machine in BoR's equipment rack capable of running said software. Any issues impeding access to the remote machine are the responsibility of technical resources at the site attempting to access the remote machine

**Access to the remote machines mentioned in this section is solely controlled by BoR and will require a different set of user credentials than the ones mentioned in the Security Policies section of this document; however, the same security policies apply.**

## Removal or Modification of Scheduled or Running Conferences by BoR

This section provides notification to participating institutions that BoR has authority over any conference scheduled or running on BoR equipment.

1. BoR, may, at its discretion, require conference reservations to be modified or removed. If BoR was not made aware of the reservation through the procedures outlined elsewhere in this document, it may be removed by BoR **WITHOUT WARNING**.
2. BoR, may, at its discretion, require running conferences to be modified or removed. If BoR was not made aware of the running conference through the procedures outlined elsewhere in this document, it may be removed by BoR **WITHOUT WARNING**.
3. Any scheduled or running class or class event determined by BoR to be causing a stability or resource issue on BoR equipment or network, will, at the sole discretion of BoR, be removed **WITHOUT WARNING** from the system. After removal, BoR may attempt to work with affected parties to remedy this situation; however if it is determined that there is no reasonable solution, the class or schedule will be permanently removed.
4. Any endpoint determined by BoR to be causing a stability or resource issue on BoR equipment or network, will, at the sole discretion of BoR, be removed **WITHOUT WARNING** from any class or event of which it is a participant. After removal, BoR may attempt to work with affected parties to remedy this situation; however if it is determined that there is no reasonable solution, the endpoint will be permanently removed.

## Appendix A: Firewall Information

This section is strictly informational and does not set forth any policies or procedures. Many participating institutions accessing BoR equipment for video conferencing have issues with being behind firewalls that do not natively pass H.323 video conferencing traffic. The following is a list of firewall ports taken from documentation found on the internet which may assist in configuring a firewall to allow H.323 video conferencing traffic through the firewall. The presence of this documentation does not imply that BoR provides any technical support concerning the configuration of any network equipment at participating institutions.

	Port(s)	Type	TCP	UDP	Purpose
<b>Common</b> (May Not Apply To All Systems or Setups)	21	Static	X		FTP for endpoint software upgrades
	23	Static	X	X	Telnet
	80	Static	X		HTTP – web interface for codec control and menus
	389	Static	X		LDAP – ILS registration
	443	Static	X		HTTPS – web interface for codec control and menus
	1300	Static	X	X	Used to secure a H.323 host call
	1503	Static	X		Used for T.120 file sharing
	1718	Static	X	X	Gatekeeper discovery
	1719	Static	X	X	Gatekeeper RAS
	1720	Static	X	X	H.323 host call using Q.931 call setup
	1731	Static	X	X	Audio call control for VoIP
	2979	Static	X	X	H.263 video streaming
<b>Cisco</b>	2326 – 2373	Dynamic		X	Available port in this range is used for exchange of H.245 call parameters (RTCP)
	5555 – 5580	Dynamic	X		Available ports in this range are used for audio and video
<b>Life Size</b>	5060	Static		X	Used for control of video calls using SIP
	60000 – 64999	Dynamic		X	Available port in this range is used for exchange of H.245 call parameters (RTCP)
	60000 – 64999	Dynamic	X		Available ports in this range are used for audio and video
<b>Polycom</b>	3230 – 3253	Dynamic		X	Available port in this range is used for exchange of H.245 call parameters (RTCP)
	3230 – 3235	Dynamic	X		Available ports in this range are used for audio and video
<b>Polycom HDX</b>	3230 – 3285	Dynamic		X	Available port in this range is used for exchange of H.245 call parameters (RTCP)
	3230 – 3243	Dynamic	X		Available ports in this range are used for audio and video