互联网仲裁推荐标准

（广州标准）

2020年9月10日发布

广州仲裁委员会

目录

[第一编 互联网仲裁开庭技术标准细则 3](#_Toc21479)

[1. 硬件 3](#_Toc6070)

[2. 软件 7](#_Toc19790)

[3. 场地标准 9](#_Toc5355)

[4. 数字安全 11](#_Toc665)

[5. 其他规范 13](#_Toc13040)

[附件《互联网仲裁在线开庭技术与实施指南》 15](#_Toc8439)

[1.硬件 15](#_Toc22571)

[1.1视频采集设备 15](#_Toc29538)

[1.2音频采集设备 15](#_Toc20786)

[1.3视频显示屏 16](#_Toc5012)

[1.4操作显示器 16](#_Toc14956)

[1.5分屏显示器 16](#_Toc14242)

[1.6路由器 16](#_Toc30643)

[2.软件 17](#_Toc10642)

[2.1视频软件 17](#_Toc12847)

[2.2音频软件 17](#_Toc8284)

[2.3安全软件 18](#_Toc21941)

[3.数字安全 19](#_Toc11833)

[3.1设备安全 19](#_Toc4721)

[3.2加密 20](#_Toc22064)

[3.3通讯安全 21](#_Toc19629)

[3.4物理与环境安全 22](#_Toc11068)

[3.5运营安全 23](#_Toc29673)

[3.6访问控制 23](#_Toc11657)

[4.环境 24](#_Toc17316)

[4.1场地 24](#_Toc32398)

[4.2仲裁机构互联网仲裁参与者环境场地示意图 25](#_Toc17291)

[4.2互联网仲裁参与者自行管理环境场地示意图 25](#_Toc2839)

[4.3设施 25](#_Toc18909)

# 第一编 互联网仲裁开庭技术标准细则

## 硬件

硬件，指在互联网仲裁过程中使用的各类数字信息输入、输出设备和以实现必要的音视频采集、文件展示、数据传输与存储以及数字安全保障等功能为目的的数据处理设备。

制定硬件技术标准的目的，是为互联网仲裁程序的合法性、系统运行的安全稳定和文书质量规范性提供基础保障，并通过对主要硬件的类型、效果和技术指标等条款的规定，达到以上目的。

硬件技术指标的具体内容，请查阅本标准附件。

* 1. 视频采集设备
     1. 视频采集设备

指可以将参与者环境现场影像转换为数字视频讯号，并将视频讯号输入至现场主机变为可处理数据的设备。

视频摄像头是互联网仲裁在线庭审过程中使用的主要的视频采集设备。

* + 1. 采集范围

视频采集范围应当包含参与者环境场地内全部人员。

* + 1. 采集质量

视频采集应满足必要的质量要求，参与者环境场地内所有人员的面部、名称标识牌、参与者环境背板与图标文字等，均应清晰可辨认。

* + 1. 遥控设备

可以使用视频遥控采集设备，对画面进行缩放及角度调整等操作。

* 1. 音频采集设备
     1. 音频采集设备

指参与者在线开庭采用麦克风录音的方式，将声音转化为数字讯号并传入参与者环境现场的计算机的设备。

* + 1. 采集范围

音频采集应当满足必要的范围要求，如实记录场地内全体人员的语音信息和证据展示的音频内容。

* + 1. 采集质量

音频采集应当满足必要的质量要求，可清晰收听、辨认场地内全部人员及厅内环境杂音。可以使用具有降噪、定向采集等功能的硬件设备，提高音频采集质量。

* 1. 互联网仲裁参与者环境终端的计算机

为确保在线开庭的有序进行，参与者环境可根据实际情况，在不影响正常使用互联网仲裁系统的前提下，自行配置计算机等硬件及系统。参与者环境的终端系统硬件及系统应当随技术升级而不断更新。

* + 1. 数据类型

参与者环境的终端系统的计算机支持接收与输出的数据类型，包括但不限于音频、视频、网络数据等。

* + 1. 文档类型

参与者环境终端系统的计算机支持处理、浏览的文件类型，包括但不限于音频、视频、图片、文字、表格、程序代码、网站页面、压缩文件等。

* + 1. 接入终端设备

参与者环境终端的计算机应当已经集成或支持接入和输出的硬件，从而保证其能完成互联网仲裁系统的使用所必须的功能，包括但不限于显示屏、音箱、摄像头、麦克风、集线器、键盘、鼠标等。

* 1. 视频显示屏

视频显示屏是网络仲裁的重要组成部分，通过与主机的连接，显示双方当事人、代理人及其他互联网仲裁参与者环境现场的在线画面。视频显示屏应当满足必要的尺寸和清晰度要求，以使仲裁员可以清晰地观看屏幕画面。

* 1. 音频播放设备

音频播放设备是网络仲裁的重要组成部分，通过与主机的连接，播放双方当事人、代理人及其他的互联网仲裁参与者环境现场的在线音频信息。

* 1. 操作显示器

用于显示互联网仲裁参与者环境主机操作界面的显示设备。

* 1. 分屏显卡

参与者环境终端的计算机应配置一个分屏显卡，以使每个显示设备可以通过主机分别获得独立的画面与操作界面。

* 1. 路由器

每个参与者环境场地内应配置至少1台专用路由器，用于连接该参与者环境的网络专线。

* 1. 防火墙

一种位于内部网络与外部网络之间的[网络安全](https://baike.so.com/doc/1276211-1349506.html" \t "https://baike.so.com/doc/_blank)系统。为确保网络安全，互联网仲裁参与者环境场地内的每条专线都应加装硬件防火墙。

## 软件

软件，指在互联网仲裁过程中使用的各类计算机系统、应用软件及数字服务，以实现必要的音视频信号转化、音视频文件生成、文件展示、数据传输与存储以及数字安全保障等功能。

制定软件技术标准的目的与硬件技术标准的目的相同，即为满足互联网仲裁程序的合法性、系统运行的安全稳定和文书质量规范性等要求提供基础保障。本标准将制定对各类软件及数字服务的约束条款。软件技术指标的具体内容，请查阅本标准附件。

* 1. 操作系统

指管理和控制计算机软硬件资源的系统软件，是互联网仲裁系统的重要组成部分，包括计算机、服务器及移动数字设备操作系统。互联网仲裁应支持在多种操作系统环境下稳定、高效、安全运行。

操作系统应当包括但不限于Linux、Windows、MacOS、麒麟操作系统、iOS、Android、Windows Mobile等广泛使用的操作系统。

* 1. 视频软件
     1. 视频采集软件

指用于视频采集设备的数字信号转化及设备遥控等应用软件，主要包括视频编解码器、压缩编解码器、摄像头遥控软件等。

互联网仲裁参与者环境应当使用成熟、稳定、高效的视频采集软件，以使生成的视频文件符合本标准的相关要求。

* + 1. 视频播放软件

指安装在主机上的，用于打开视频格式文件的播放器软件。参与者可根据实际情况，安装一个或多个视频播放软件，以满足仲裁过程中各种视频文件类型的展示需求。

* 1. 音频软件
     1. 音频采集软件

指用于音频采集设备的数字信号转化应用软件，主要包括音频编解码器、压缩编解码器等。

互联网仲裁参与者环境应当使用成熟、稳定、高效的音频采集软件，以使生成的音频文件符合本标准的相关要求。

* + 1. 音频播放软件

指安装在主机上的，用于打开音频格式文件的播放器软件。参与者环境可根据实际情况，安装一个或多个音频播放软件，以满足仲裁过程中各种音频文件类型的展示需求。

* 1. 通讯软件

指在互联网仲裁过程中所使用的通讯软件，包括但不限于即时通讯软件、视频会议系统、数据传输工具等。在互联网仲裁过程中应使用安全、合法的通讯软件，避免使用无授权通讯软件。

* 1. 安全软件

指具有操作系统或应用软件安全保护功能的软件或服务，是保障互联网仲裁安全性的重要组成部分。互联网仲裁过程中所使用的各类终端设备，均应安装安全软件，并定期更新和运行。

* 1. 其他软件与服务

在互联网仲裁过程中还会使用到各类其他软件和服务，如输入法、浏览器、云存储客户端、办公软件、加解密软件等，互联网仲裁参与者环境应在确保软件安全性的情况下，使用必要的软件与服务，禁止安装、使用与互联网仲裁无关的软件和服务。

## 场地标准

制定环境标准的目的，是通过对互联网仲裁参与者的场地、环境、设施等内容的约束条款，强化互联网仲裁程序合法性，维护互联网仲裁参与者环境秩序，保障互联网仲裁各类文书、文档质量。

环境标准指标的具体内容，请查阅本标准附件。

* 1. 场地

互联网仲裁参与者环境应为仲裁员、仲裁秘书等处于该环境内互联网仲裁参与人员提供至少一个独立的物理空间，用于放置互联网仲裁终端设备、推进互联网仲裁程序、维护互联网仲裁参与者环境秩序以及编辑仲裁文件。

互联网仲裁参与者环境场地应满足必要的条件，以使互联网仲裁满足本标准相关条款要求。

* 1. 环境
     1. 指由仲裁机构提供的参与者环境现场，应以包含仲裁机构名称全称的背景板或背景墙作为背景。
     2. 参与者环境现场，应使用标牌注明仲裁参加人员的身份（仲裁员、秘书等）。
  2. 设施

互联网仲裁参与者环境场地应具备必要的基础设施，以保障仲裁过程正常、有序进行。

* + 1. 照明设备

参与者环境应具备充足的光源，以保障整个开庭过程中当事人/代理人和仲裁员互相可以清晰地看到对方。

* + 1. 电力设备

互联网仲裁系统运行硬件设备所在地以及每一个参与者环境应当保证良好的供电环境，其中互联网仲裁系统运行硬件设备所在地应当有预备应急电源和多种网络接入，防止因停电导致的断网或其他影响庭审进程的情况发生。

* + 1. 监控设备

参与者环境现场，应具备安防监控系统的前端和传输设备，并确保对整个仲裁进程进行全方位无死角实时监控。监控设备参数，如图像质量等级、水平清晰度、灰度等级、信噪比等，应符合仲裁活动开展所在地国家、地区安全防范报警设备及系统相关规定。

* 1. 网络
     1. 互联网仲裁系统运行的硬件环境应配置适当的硬件设备，确保在开庭过程中可以稳定、持续地接收和发送数据信息。
     2. 互联网仲裁参与者环境应同时支持有线网络和无线网络两种方式以便不同参与者到场参加互联网仲裁活动。
     3. 每个参与者环境应配置至少一条网络专线，专线应具备较高的网络速度，以满足本标准对互联网仲裁系统各环节的质量要求。
     4. 互联网仲裁参与者环境应为场地内的双方当事人及其他非工作人员提供专用且安全的网络环境。

## 数字安全

制定数字安全标准的目的，是通过对各种技术和管理措施加以规范约束，保障互联网仲裁系统正常运行，维护互联网仲裁程序的合法性，系统数据的可用性、完整性和保密性。

本标准将通过对数字安全相关的加密信息类型、加密技术、通讯、物理与环境安全和运营安全等方面制定约束性条款，保障系统数字安全。安全措施和技术指标的具体内容，请查阅本标准附件一。

* 1. 数字安全的总要求

任何仲裁参与者对仲裁信息安全性方面的任何破坏都可能损害整个仲裁的安全性。因此，仲裁程序中信息的安全性最终取决于所有相关个人的决定和行动。任何人的行为都可能是信息安全事件 “最薄弱的环节”，安全事件往往由于个人行为不当而非系统设计瑕疵。

在系统性信息安全保障制度实施的同时，任何仲裁参与者均应提高信息安全意识，规范个人行为。

* 1. 数字信息类型

以下数字信息具有较高的安全特性，应当重点加以保护：

1. 个人信息数据，如姓名、身份证件信息、通信方式、居住地址等；
2. 敏感数据，如健康信息、用药记录、病历记录、犯罪记录、银行及个人财务记录、银行卡信息等；
3. 商业机密，如财务或会计记录、流水单、商业文件等；
4. 涉及专有数据库或其他具有独立价值的数据；
5. 未经公开的协议或其他法律文书；
6. 知识产权信息；
7. 其他可能对个人、商业组织、政府或社会公众利益造成影响的非公开信息。
   1. 安全知识与培训

互联网仲裁系统的管理者应紧跟安全威胁和解决方案趋势。维护数字安全性是一个持续的过程，应建立有效的风险预警机制，保障系统安全性。

互联网仲裁的参与者及相关人员，应履行保护网络与数字安全的义务，应定期参加培训，学习保护数字信息机密性、完整性和可用性的法规与相关措施。

* 1. 设备与数据的安全管理机制

建立完善的互联网仲裁设备安全机制，提高互联网仲裁安全性，包括但不限于对硬件、软件、知识产权、数据及电子文档的安全性保护。

* 1. 信息加密

加密是使用算法转换信息以使未经授权的人无法读取相关信息的过程，是保障互联网仲裁安全性措施的重要组成部分，应对互联网仲裁过程中的重要环节进行加密处理，包括但不限于文件加密、硬盘加密、数据传输加密、云加密、在线音视频加密等。

* 1. 通讯安全

建立完善的通讯安全机制，避免网络攻击，是互联网仲裁安全、稳定运行的基础，包括但不限于防范网络钓鱼、文件共享与存储安全及网络服务安全等措施。

* 1. 物理与环境安全

控制对信息资源的物理访问，以防止未经授权的访问、损坏或干扰，防止设备丢失或被盗。包括但不限于便携式存储设备安全及视觉黑客防范等措施。

* 1. 运营安全

制定并执行完善的互联网仲裁运营安全规范，避免在运营过程中产生的安全隐患，包括但不限于软硬件使用规范、账户管理办法、数字围栏等方面的安全隐患。

## 其他规范

* 1. 应急预案

在互联网仲裁过程中，互联网仲裁终端系统应当针对一些突发事件提前做好预案准备。包括但不限于以下情况：

* + 1. 因停电、断网等事故导致无法传输网络数据或视频数据；
    2. 因设备问题导致庭审视频画质严重下降，模糊不清，从而导致工作人员无法正常记录，庭审中断；
    3. 因仲裁员、办案秘书或当事人突发状况，庭审无法继续进行；
    4. 其它导致庭审中断的情况。

# 附件《互联网仲裁在线开庭技术与实施指南》

## 1.硬件

### 1.1视频采集设备

1.1.1视频采集设备应连接至参与者环境场地内的主机，并可将采集到的音视频数据成功输出到主机。

1.1.2可以使用多视频源接入方式，将场地内多个视频采集的视频信号展示在同一操作显示器上。

1.1.3为达到更好的视频采集效果，参与者环境可以使用数字摄像机或具有视频采集功能的数字照相机等设备。

1.1.4视频采集设备应具备不低于80度的广角镜头。

1.1.5视频采集设备分辨率不低于1080P。

1.1.6视频采集设备应支持4:3或16:9的画面比例。

1.1.7视频采集设备应置于适当的位置，以使画面包含双方当事人、代理人、仲裁工作人员等面部及肩部以上部位。

### 1.2音频采集设备

1.2.1音频采集设备支持的声音频率范围为20Hz～20kHz。

1.2.2音频采集设备接线口应当为卡农接口或6.5mm同轴音频插头。

1.2.3集线器

当多个自然人在同空间内同时参加仲裁活动时，应当为每一个自然人配置一个音频采集设备，当现场布置多个音频采集设备时，可使用集线器将多个音源数据统一输出到指定终端设备，达到多重音频采集的效果。

### 1.3视频显示屏

1.3.1参与者环境应根据场地情况，配置2台尺寸不小于55英寸，具有HDMI或其他类型高清输入接口的高清电视机。

### 1.4操作显示器

1.4.1不少于2台操作显示器。

1.4.2辨析率不低于1024\*768。

1.4.3输入接口为HDMI或其他类型的高清视频数字接口。

### 1.5分屏显示器

1.5.1 分屏显示设备应具备不小于同时连接4个视频显示屏的接口。

1.5.2 分屏显示设备应具备持HDMI和VGA接口。

### 1.6路由器

1.5.1具备静态地址分配功能

1.5.2可以自动切换信道

1.5.3支持5GHz或波束成形技术

## 2.软件

### 2.1视频软件

#### 2.1.1视频采集软件

2.1.1.1可以采用开源框架，支持Web端或移动端的在线开庭。

2.1.1.2可以使用分层编码传输控制技术、丢包恢复（PLC）等视频处理技术，保障在线视频的流畅度和质量。

2.1.1.3可以使用MPEG4 、H263、H263+、H264等编解码技术。

2.1.1.4视频封装过程中，禁止对庭审的画面、音频、时间轴等内容信息进行任何修改。

2.1.1.5可以使用视频遥感软件，在保障画面内容符合本标准相关规定的前提下，对视频采集设备的方向、广角、曝光度等参数进行调整。

#### 2.1.2视频播放软件

2.1.2.1支持播放WMV、ASF、SWF、FLV、AVI、MPG、MPEG、DVD、RM、RMVB等格式的视频文件。

2.1.2.2网页浏览器可以作为视频播放软件使用。

### 2.2音频软件

#### 2.2.1音频采集软件

2.2.1.1庭审现场的音频数据与视频数据，应达到可以独立采集的标准。

2.2.1.2独立采集的音频数据与图像组合成视频数据时，应确保音视频数据时间戳显示时间一致。

2.2.1.3可以使用音频自动增益补偿（AGC）、噪音抑制（ANS）、回声消除（AEC）、静音检测（VAD）等技术，提高音频质量。

2.2.1.4音频采样率应不低于22.05KHz

2.2.1.5禁止在音视频采集阶段使用诸如消声、变声、噪音增强等技术降低音频识别度。

#### 2.2.2音频播放软件

2.2.2.1支持播放CD、WAV、WAVE、AIFF、MP3、MIDI、WMA、Realaudio、APE、FLAC、AAC等格式的视频文件。

2.2.2.2网页浏览器可以作为音频播放软件使用。

### 2.3安全软件

2.3.1安装病毒防护软件，实现对实时运转的业务系统进行计算机病毒、木马和恶意程序的查杀，并能够及时进行病毒库升级，设置合理的病毒查杀防范策略。

2.3.2安装系统防护软件，实现对所有终端设备、服务器操作系统、应用软件等安全监测和防护，能够采用白名单机制，阻止未经授权的运行或访问，设置合理的安全策略，保障最小化安全原则。

2.3.3安装文档管控软件，针对系统中所使用的文件采用分级方式实现对文档使用、存储、转发、追朔等管理。

2.3.4安装安全审计软件，针对系统运行情况，进行信息收集、整理、分析和展现，监控系统运行情况和发现异常情况。

2.3.5加密管理和使用系统，实现对密钥的管理，提供符合仲裁活动开展所在地国家规定加密运算机制。

## 3.数字安全

### 3.1设备安全

3.1.1仲裁委员会及相关仲裁人员，应了解其数据安全基础架构，了解数据流及存储位置。包括：专用和个人网络以及网络设备（例如路由器和防火墙），计算机，平板电脑，智能手机以及其他便携式设备（例如USB驱动器）），计算机设备（例如打印机，扫描仪，支持Internet协议的视频和安全设备，传真机），云服务，软件程序和应用，远程访问工具以及备份服务。

3.1.2最大程度地减少未经授权的用户访问敏感数据的风险，禁止与没有权限的个人或机构共享数据。

3.1.3建立访问报警机制，并通知未经授权的一方删除相关数据。

3.1.4避免不必要的多份数字文档副本，定期查找并安全处理多余副本，尤其注意清理电子邮件传输及“下载”文件夹中产生的不必要的数字文件副本。

3.1.5互联网仲裁参与者环境所使用、生成、存储的各类文书或文件，应当是同一文档副本，避免不必要的文档副本。

3.1.6互联网仲裁生成的音视频资料，自结案之日起，需保存10年以上。

3.1.7鉴于庭审过程中会同时出现多端多用户视频信息流，故同一庭审的视频文件，应存储在一个文件夹或压缩包中，且该文件夹或压缩包的名称，应以固定格式自动生成或手动设置。格式可以是“仲裁机构缩写+开庭日期+互联网仲裁案件号”，如“GZAC201911121912CCCM90021”。

3.1.8庭审视频一经生成，其对应的全部视频文件及文件夹，在规定时间内不可被删除、更名或替换。视频存储文件的每一次操作，都应记录在相应的操作日志当中。

3.1.9建立文件保留和销毁日志，禁止对数据进行匿名处理。

3.1.10为数字设备和文件提供安全、可靠的保存介质和环境。

3.1.11互联网仲裁所使用的终端系统的软件与设备，可以使用远程位置跟踪及数据擦除功能，包括手机、平板电脑、笔记本电脑在内的移动设备。

3.1.12记录数字设备使用场所的变更情况。

3.1.13进行常规的安全和冗余数据备份，以避免数字文件损毁带来的不可恢复损失。

### 3.2加密

3.2.1加密数字传输

数据在未受保护的Wi-Fi网络或基础互联网数据传输协议下，存在较大的安全风险。互联网仲裁在数字传输过程中应尽量使用安全级别更高的传输协议或体系。如VPN网络、端到端加密传输或使用HTTPS安全性的网站。

3.2.2文件级加密

可以在传输特定文档或文件夹之前对其进行加密。许多流行的应用程序（例如Microsoft Office文档、PDF文档、文件压缩工具等）都提供了向文件添加密码以加密其内容的选项。

建议优先使用中文字符对文件进行加密。

3.2.3全盘加密

为了防止由于主机或其他设备的丢失而导致未经授权的数字信息访问，可以使用全盘加密，以保护设备的整个硬盘驱动器免受未经授权人员的侵害。

3.2.4云加密

在将数据上传到文件共享或云存储服务之前，先对其进行加密。

避免使用免费的文件共享或云存储服务，因为这些免费服务的安全性较弱，应尽可能地使用具有较高安全性的云服务。尽量使用具有两个加密密钥才能解密、加密的数据云存储服务，该类服务为用户提供了密钥的唯一保管权，而非与云提供商共享，即使云服务本身遭受了安全威胁，入侵者也将无法访问用户的数据。

### 3.3通讯安全

3.3.1附件和链接

网络钓鱼是比较常见的网络攻击，通过模仿已知或被授权的来源进入数字系统，危害数字安全。禁止互联网仲裁人员从未知的来源下载程序和数字信息，更不要打开未知来源的附件和网站链接。

非仲裁委员会自有数据系统的数据来源，均应默认为未知来源。

应在互联网仲裁连接的各类数据终端安装反钓鱼或防病毒软件。

3.3.2使用安全度较高的文件共享或云存储服务替代电子邮件，以实现更加安全的文件传输。

3.3.3尽量避免使用公用网络。

当事人及仲裁人员应优先使用仲裁委员会提供的专用网络或VPN网络环境，或使用已被保护的Wi-Fi网络环境。如无法使用以上网络环境，应优先使用个人手机蜂窝热点。

### 3.4物理与环境安全

3.4.1便携式存储设备的风险

便携式存储设备（如USB硬盘）体积小且操作简便，是数字文件和恶意软件传送的常规途径。

互联网仲裁过程中使用的主机及各连接终端，应对接入的移动存储介质进行实时的安全扫描和查杀。如有必要，应禁止主机及各连接终端连接移动存储设备。

3.4.2锁定设备

不使用主机或连接互联网仲裁数据系统的其他数字终端时，应当关闭并锁定设备，并使用电缆锁或扩展坞。

3.4.3防范视觉黑客

在异地办公或公共场所访问数据信息或使用数字账户时，应为终端设备设置隐私屏幕。

### 3.5运营安全

3.5.1尽量避免使用免费或安全性较低的数字服务，例如电子邮件服务，云共享文件服务，虚拟专用网络和防病毒软件。

3.5.2禁止共享设备和账户给非仲裁人员及与案件无关的人员使用。

3.5.3保护数字围栏，使用诸如防火墙、防病毒及反恶意软件、防间谍软件等围栏保护措施。

3.5.4及时安装软件更新和补丁。

3.5.5监控漏洞

仲裁员和仲裁委员会应在每次使用时注意终端软件环境的安全有效性，采取措施纠正或减轻安全弱点，并有义务提示当事人提高安全意识，执行安全操作。

### 3.6访问控制

3.6.1使用符合仲裁活动开展地所在国家、地区与商业秘密或密码等有关的法律法规所规定的密码保护技术或具有高度安全性的数字验证系统，如密码管理器、Hash算法、区块链及指纹、面部识别、视网膜扫描等生物识别技术。

3.6.2建立密码变更间隔机制，仲裁人员及系统管理人员的密码应至少3个月变更一次。

3.6.3登录系统或访问数字信息时，可通过手机短信、电子邮件或电子令牌等渠道向访问者发送特殊代码，提高身份识别的安全性和准确性。

3.6.4访问权限变更日志，记录访问权限的变更时间和变更内容，及时更正权限错误，发现安全隐患，降低访问权限风险。

3.6.5互联网仲裁参与者环境应当严格控制访问权限，并且可以及时终止无权访问。

3.6.6记录并保留主机操作日志。

## 4.环境

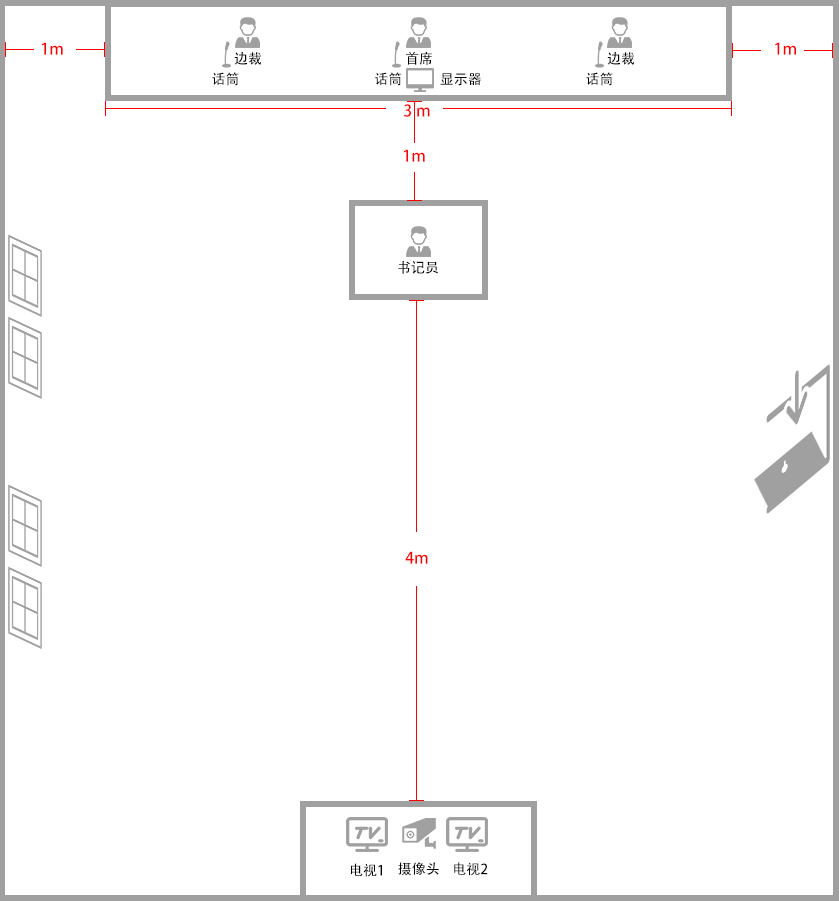
### 4.1场地

4.1.1参与者环境场地应为不低于40平方米的长方形庭室，长不低于8米，宽不低于5米。

4.1.2鉴于仲裁的不公开原则，庭审的声音不应被外界听到，庭审的过程也不应受外界的声音的影响，因此要保障参与者环境场地的隔音效果。

4.1.3每个参与者环境场地内在一个时间段内只允许进行一个仲裁案件庭审。

### 4.2仲裁机构互联网仲裁参与者环境场地示意图



### 4.2互联网仲裁参与者自行管理环境场地示意图

待补充

### 4.3设施

4.3.1照明设备

参与者环境应具备充足的光源，以保障整个开庭过程中当事人/代理人和仲裁员互相可以清晰地看到对方。

4.3.2电力设备

在线庭审中，当事人是通过网络的渠道介入，因此要保证供电及网络正常，并预备应急电源和多种网络接入，防止因停电或者断网影响庭审进程。

4.3.3监控设备

参与者环境现场，应具备安防监控系统的前端和传输设备，并确保对整个仲裁进程进行全方位无死角实时监控。监控设备参数，如图像质量等级、水平清晰度、灰度等级、信噪比等，应符合仲裁活动开展所在地国家、地区安全防范报警设备及系统相关规定。