

## 2021 年运训单招成都体育学院考点考务系统

### 租赁服务合同

合同编号: C72C202/022

签订地点: 成都

甲方(承租方): 成都体育学院

乙方(出租方): 武汉铭德相合投资管理有限公司

根据《中华人民共和国合同法》以及成都体育学院相关校内采购制度,经甲、乙双方协商一致,同意签订本合同。详细技术说明及其他有关合同项目的特定信息由合同附件予以说明,合同附件为本合同不可分割的部分。双方同意共同遵守如下条款:

#### 一、租赁要求

1、本次体考统考时间为:2021年4月27日-2021年4月30日,乙方应按甲方要求提前进场,2021年4月25日前完成软、硬件设备的安装、调试,并参加4月26日的现场打分培训,确保考前准备工作到位。

2、乙方提供的考试系统应完全满足甲方的需求,且为整体打包服务(包括满足本次考试的软件、硬件、耗材、技术服务等),乙方全力保障甲方的考试工作,针对田径、羽毛球、体操、艺术体操4个项目分别安排技术人员进行全程的技术支持。

3、乙方提供的本次服务中涉及到的软件、硬件,均应采取充分的安全措施,做好保密工作,凡对触及到的本次体考的考务人员、考生以及其他与本次考试相关的人员信息、考试数据信息、考场情况等信息,均不得泄露,若因乙方软件、硬件设备遭到攻击或其他乙方因素导致的数据破坏、数据泄露等事故,由乙方承担一切责任和损失。

5、详细的服务要求见附件。

#### 二、合同价格

本租赁合同单价按照30元/人计,此单价为包含软件、硬件、技术人员的服务、差旅、食宿以及税费等的综合单价。

费用预计:2568\*30元/人=77040元

最终报价：因项目首次使用，且时间紧张，相关配套软件属于沟通协调开发阶段，导致个别需求无法短时间满足。所以最终价格调整为：49800 元。该价格为完成本合同约定服务的所有费用，除另有补充约定外，超过本价格的其他费用，甲方不予支付。

### 三、其他要求

1、乙方提供软件、硬件设备应是完好的，良好运行的，且权属清晰，不得侵害他人的所有权。

2、乙方提供的现场技术服务人员应当专业技术性强，能够满足甲方考试现场设备、系统的及时维护。若所派技术人员专业素养低，不能承担甲方现场设备、系统维护的，甲方有权拒绝支付服务费用，若给甲方造成损失的，甲方有权追究乙方违约责任。

3、设备（含软件）必须符合国家相关标准，保证考试数据准确性和安全性。

4、设备（含软件）出现问题，乙方应负责三包（包修、包换、包退），费用由乙方承担。

5、乙方所派技术人员（含负责人）在考试现场，视为相关考务人员，其言论、行为受到国家相关考试法律法规及考试制度的约束，相关责任由乙方所派技术人员自行承担。

6、保密约定：乙方在服务过程中，凡接触到的与体考有关的任何数据、信息，均不得泄露；凡未经官方公布的与体考有关的新闻、图片、视频等，均不得擅自公开（包括在 QQ、朋友圈、公众号等网络媒体上公开）。否则，视为乙方严重违约，甲方有权追究乙方违约责任，且乙方须承担由此造成的一切损失。

### 四、付款方式

1、租赁服务完成后，乙方须向甲方提供合法有效完整的完税发票及凭证资料。因发票不合格或瑕疵给甲方造成的一切损失（包括但不限于税务损失）由乙方承担。甲方至收到乙方相关发票及凭证资料之日起三十日内完成支付结算。

### 五、违约责任

#### 1、甲方违约责任

(1) 甲方无正当理由不接受本次租赁服务的，甲方应偿付合同总价百分之三十的违约金；

(2) 甲方偿付的违约金不足以弥补乙方损失的，还应按乙方损失尚未弥补的部分，支付赔偿金给乙方。

(3) 甲方未按规定时间付款的，甲方应该支付合同总价百分之三十的违约金给乙方。

(4) 因新冠病毒疫情原因考试不能如期或其他政策原因改变考试方式而不能实施本次租赁服务的，甲方不予承担违约责任。

## 2、乙方违约责任

(1) 乙方交付的服务质量不符合合同规定或乙方所供设备（含软件）及所含配件非正品的，乙方应向甲方支付合同总价的百分之三十的违约金，并须在甲方规定的时间内更换合格的设备给甲方，否则，视作乙方不能交付服务而违约，按本条本款下述第“(2)”项规定由乙方偿付违约赔偿金给甲方。同时甲方有权通过法律途径追究乙方相关法律责任。

(2) 乙方不能按甲方要求提供设备（含软件）和相关服务，且不能提供及时的应急服务，导致甲方考试不能顺利进行的，视为严重违约，甲方有权终止合同，不得支付乙方任何费用，乙方还应承担合同暂定总价百分之三十的赔偿金，且乙方3年内不得参加甲方的任何采购活动。

(3) 若乙方设备（含软件）、服务不符合甲方租赁要求的，视为乙方没有按时交货而违约，乙方须在两天内无条件更换合格的设备（含软件）和服务，如逾期不能更换的，甲方有权终止本合同，乙方应另付合同总价的百分之三十的赔偿金给甲方。

(4) 乙方保证本合同设备（含软件）以及服务的所有权及知识产权等权利无瑕疵。如任何第三方经法院（或仲裁机构）裁决有权对设备（含软件）主张权利或国家机关依法对设备进行没收查处的，乙方除应向甲方返还已收款项外，还应另按合同总价的百分之三十向甲方支付违约金并赔偿因此给甲方造成的一切损失。

(5) 乙方偿付的违约金不足以弥补甲方损失的，还应按甲方损失尚未弥补的部分，支付合同结算总价百分之三十的赔偿金给甲方。

## 六、争议解决办法

1、因设备(含软件、)服务的质量问题(包括考试数据的准确性)发生争议,由相关行政监管部门或其指定的鉴定机构进行质量(含数据准确性)鉴定。符合标准的,鉴定费由甲方承担;不符合质量标准的,鉴定费由乙方承担。

2、合同履行期间,若双方发生争议,可协商或由有关部门调解解决,协商或调解不成的,双方均可向甲方所在地有管辖权的法院提请诉讼。

## 七、其他

1、本合同自双方法人代表或授权代表签字盖章后立即生效。

2、合同执行期内,双方均不得擅自变更或解除合同,合同如有未尽事宜,需经双方共同协商,做出补充规定,补充规定与本合同具有同等法律效力。

3、合同附件(包含乙方的报价承诺)为本合同的组成部分,与本合同正文具有同等法律效力,若合同附件与合同正文有任何冲突,以对甲方惠利更大的为准。

4、本合同一式四份,甲、乙双方各执二份,具有同等法律效力。

附件:具体服务要求

甲方:成都体育学院(盖章)

法定代表人(授权代表):

单位地址:成都市武侯区环环路西段19号

开户银行:建行成都青羊支行

帐号:51001446436051506118

纳税人识别号:12510000400008116Y

电话:028—85097065

传真:

签约日期:2021年5月10日

乙方:(盖章)武汉铭德相合投资管理有限公司

法定代表人(授权代表):

单位地址:湖北省武汉市洪山区佳园路光谷国际商会大厦

开户银行:中国银行股份有限公司武汉喻园支行

帐号:559962243437

纳税人识别号:91420100070538391M

电话:马强,17629009503

传真:

签约日期:2021年5月10日

**附件：具体服务要求**

**内容：系统+技术人员全程服务**

### **一、软件类开发及技术服务要求**

系统主要软件应该为供应商自行开发、具有底层代码修改权限的成熟软件系统。对于采购所需的相关常见软件功能，应该有成熟的模块及相关的界面，供应商应该同时提供相关界面的软件系统截图。

#### **1、考生信息管理系统**

具有完善的考生综合信息管理、信息改动日志记录及回溯模块、信息修改权限管理功能、信息导入导出功能、考生信息的有效性严谨校验功能等相关功能。该信息系统应具备管理不少于至少 5 年总考生数量的全部考生信息的信息容量（即不少于每年 150 万条数据管理），并可以根据需要随时查阅、检查往年的考生报名数据。

同时要求该系统提供商能提供不少于 100 万条真实信息的测试及演示，确保在高达 5 年的总考生数据情况下，系统依旧可以快速的完成各项功能。

#### **2、报表统计功能**

能根据考试考务工作需要，实时提供关于考生最新报名人数、分科类报名人数、分地区报名人数、重复报名人数排查等相关的报表统计功能。

报表功能的实现，要求基于浏览器，而不需要管理员安装特定的软件、插件、控件等，只需浏览器即可完成报表的生成及下载。同时报表同时应支持网页版及 OFFICE 版两种类型的格式，以方便使用。

#### **3、权限管理功能**

考务系统应有清晰、明确的分层次的多层级（四层）权限管理功能。同时应

有良好的解决方案解决未来多年的不同年度考生信息如何统一设置权限及管理。不同年份的考生数据，应该在同一个逻辑架构体系下进行管理。

#### 4、面试类考试相关管理功能（现场考试）

考务系统应该具有考场编排、考试过程相关的考题管理、交接管理等考试相关的统计、管理功能。同时应该支持包括考点管理、考场管理、不同科目及场次的考试管理功能，并且支持让报名考生自助在网上进行准考证的打印、查分等辅助功能。

针对面试考试功能，提供全套的面试考试所需的功能，包括各专项考试报名、专项考试考场编排、考生抽签、专项考试的测试数据录入、专项测试的打分及统计等考试成绩打分、录入功能。考官抽签、考官打分等考试相关的功能，功能应该成熟、可靠，确保信息的安全性及稳定性，达到性能指标。

供应商提供的考试管理功能应具备完善的考试过程管理、考试成绩核查、考试打分等完整功能，并且至少曾应用于省级以上面试的过程，以确保稳定可靠性。

## 二、硬件类租用、运维类技术服务要求

供应商应该为我校本次的考试服务，提供全部硬件设备的租赁。报价中应包含所有用到的硬件设备的租用费用。

### 1、软件系统测试服务器、备用服务器的租用。

供应商应提供软件系统所需的测试服务器、备用服务器。并可根据采购方需求，提供全部软件系统所需要的硬件服务器租用、服务器接入费用、服务器安全运维技术服务。并需要将如下设备根据采购方需要，为考试运至现场：

其中包括：

服务器硬件（2U，双路，E5-2699 v4 及以上 CPU，256G 内存）8 台

工作人员及操作人员用电脑：上限不超过 250 台

报价中应包含应采购方需要，可提供一个骨干机房的独立机柜的租用费用  
(含 300M 独享带宽)

## 2、考试现场所需硬件设备

供应商应提供考试现场所需的如下全部设备的硬件租用(以备每年的现场考试使用，需要在中标后 1 周根据采购方需求送达到位)：

(1) 考试所用到的全部电脑设备。设备总数量峰值不超过 250 台。

(2) 考试所用到的全部打印设备(含 A4 幅面打印机、高速标签打印机、热转印高速标签打印机)及全部打印耗材(碳粉、纸张等)。设备总数量峰值不超过 200 台。

(3) 现场确认拍照所需的摄像头、补光灯、背景板等设备。设备总数量峰值不超过 150 台。

(4) 考试所用到的网线、接线板、指示牌、安检门(手持安检仪)等设备。满足峰值不超过 30 个考生入口的数量要求。

## 3、考试专用设备。

(1) 供应商应提供笔试阅卷所需要的试卷扫描仪的租用。峰值数量不少于 40 台。

(2) 供应商应提供如项目所需的计时、测距等设备的租用服务。

(3) 供应商应提供面试类考试的考官用打分器设备、成绩录入设备等。其中面试打分器峰值数量不低于 300 台。

## 4、考场现场布置及技术服务人员

供应商应派驻人员在每次考试时负责考场的布置、设备的安装调试、设备的

运输及搬运、考试过程中的巡回答疑、考试现场技术服务(报价含外地考试交通、住宿费,含本地考试的工作餐、市内交通费。)

### 三、技术服务要求及产品技术性能要求

#### 1、技术服务要求

(1) 确保考试信息系统的正常使用,及时排查系统运行期间出现的各类故障,确保工作顺利开展。

(2) 确保期间的各项数据安全与保密工作,不得出现任何信息泄露的情况。

(3) 人员技术保障到位,开展好技术咨询与解答工作,及时解答报名管理人员发现的问题。

#### 2、系统架构设计要求

供应商提供的系统全套软件,应同步提供支持自动双机热备份、多机负载均衡、分布式数据库服务器的服务器设置解决方案。

要求可以实现在至少 2 个独立机房,有可以自动互相热备份的服务器及数据库服务器,确保系统的可靠性。

#### 3、并发数量性能指标:

(1) 考生总信息管理能力:不少于 750 万人。

(2) 考试并发处理能力:每日不少于 150 万人次,该 150 万人考试可在同一个时间同时开始。通过数据库集群实现数据库写入处理能力不低于每分钟 150 万条。

(3) 考务系统可实现 24 小时不间断运行,每月计划内停机维护时间不多于 2 个小时。

(4) 考试分数查询最大并发值:不低于 150 万人/秒。



(5) 主用、备用系统切换时间：正常情况下切换不多于 10 分钟。

(6) 灾难恢复时间：如遇地震、机房火灾等极特殊情况需要重新建立服务器集群，不超过 24 小时。

#### **4、硬件类设备要求：**

(1) 普通电脑：需为满足实际需要的电脑，CPU 不低于 i3 级别，内存不小于 4G。

(2) 服务器补充配置：硬盘（支持磁盘阵列）不少于 20T 的净容量。

#### **四、考试数据安全的长效机制要求**

1、全部考生数据在考试结束后必须全部清空，不得保存留档，不得用于除招生考试外的其他用途。否则，视为违约，情节严重者，将追究泄密方的法律责任。

2、考生的成绩以及个人数据需限定白名单防火墙策略，仅院校指定的服务器可下载考试视频，下载到本地的视频数据仅管理员有权限查看，评分过程即可以完全使用封闭的评分系统，也可以在学校局域网环境进行，评分过程产生的所有数据可以均在校本地，防止外网攻击；

3、工作人员访问痕迹均有日志记录，不可删除，可有效追踪管理。

#### **五、涉密信息补充要求**

**(一) 涉密信息的保密情况**由相关技术负责人直接对接协商确定，完成网上报名系统、现场拍照及确认系统的要求。供应商要对涉及到的数据进行严格的保密，现特进一步达成如下保密事项（包括技术信息和经营信息）：

- 1、供应商不得刺探与系统服务、数据管理工作无关的秘密；
- 2、供应商不得向不承担保密义务的第三方披露采购方的业务秘密，包括业务运作模式、政策情况等；
- 3、供应商不得擅自修改、备份、恢复、拷贝数据，不得向外界透露考生报名信息数据信息；
- 4、供应商如发现秘密被泄露或者由于自己过失泄露秘密，应在发现后及时采取有效措施防止泄密进一步扩大，并及时向采购方报告。
- 5、涉密人员范围：供应商参与项目的有关人员。
- 6、保密期限：1年
- 7、泄密责任：如果供应商不履行保密条款所规定的保密义务，供应商应当承担违约责任，且采购方有权追究供应商有关人员泄密的法律责任。

## **(二)、采购方机密信息包括：**

- 1、供应商能接触到采购方考试考生相关个人信息；
- 2、供应商能接触到采购方考试考务工作人员相关个人信息；
- 3、供应商能接触到采购方考试考务工作细则规定、操作日志等内部文件；
- 4、供应商能接触到采购方各类统计报表；
- 5、供应商能接触到采购方各类会议记录、讨论记录，通报的内部文件；
- 6、供应商能接触到采购方各类管理技术信息及资料；
- 7、供应商能接触到采购方所有的系统的管理员账号、密码，服务器、交换机、路由器等设备的用户名和密码口令。
- 8、供应商能接触到采购方网络系统集成的文档包括：路由器、交换机和服务器参数、网络拓扑图、网络布线图、虚网划分、IP地址分配等网络机密资料。
- 9、供应商能接触到采购方随机赠送的服务器、网络通信设备携带的说明书、各种文字资料等网络系统的重要资料。

10、供应商能接触到采购方有关网络建设与信息化建设的各种合同，上级部门的各种批文，网络管理和配备的各种规则、条例等文字材料。

11、供应商能接触到采购方达到国家规定的保密、机密、绝密级的信息。

12、其它供应商能接触到经采购方书面确定应当保密的事项。

**(三) 供应商对机密信息的保密义务包括：**

1、供应商不得以任何形式泄露采购方所提供的数据，也不得转售，否则赔偿因此造成的损失。

2、供应商在向采购方提供服务的工作中制作的资料、文件、报表等文件内容，均属采购方所有，禁止私自复制及保留副本（经采购方允许的日常工作除外）。

3、供应商需对采用电脑技术存取、处理、传递的采购方机密资料负保密责任。

4、供应商工作人员离岗离职时，应将工作时使用的电脑、U 盘等其他一切存储设备中于工作相关或与信息中心有关的信息、文件等内容交接给本部门领导，不得在离岗离职后以任何形式带走相关信息，并签署《离岗人员保密承诺书》。

5、供应商同意并承诺，无论任何原因，服务终止 100 天后，供应商不可恢复地删除服务器上的任何保密信息，并不留存副本；供应商保证退回采购方保存在供应商服务器上的任何含有保密信息的文件或资料。

6、保密义务不适用于如下信息：

(1) 非由于供应商的原因已经为公众所知的；

(2) 经采购方同意，由供应商合作的第三方知晓的信息不受保密协议限制；

(3) 由于供应商以外其他渠道被他人获知的信息，这些渠道并不受保密义务的限制；

- (4) 由于非双方可控的技术漏洞爆发所导致的非供应商可控的原因导致;
- (5) 可以从其他渠道被他人获知的信息, 这些渠道并不受保密义务的限制;
- (6) 由于法律的适用、法院或其他国家有权机关的要求而披露的信息。

7、数据操作人员授权名单由采购方提供。

8、供应商承诺在履行合同时不会进行有损采购方形象、声誉等的行为;

9、供应商承诺, 向采购方提供的内容、资料等不会侵犯任何第三方权利;  
若发生侵犯

第三方权利的情形, 由供应商承担全部责任。

10、采购方对违反上述任何一项义务的供应商保留将侵犯采购方上述秘密情节严重、构成犯罪的供应商直接工作人员移交司法机关追究刑事责任的权力。

## 六、本项目需符合以下安全保障规定:

### (一) 考试数据安全

- 1、考试全程采用实时数据实施公布的方式进行。
- 2、考试成绩上传、下载过程均加密处理, 防止考试成绩编辑、篡改;
- 3、考官提交完的考试成绩, 严格模式为打分器本地一直不留存(或宽松模式为即时删除不留存), 确保考试成绩不外泄;
- 4、存储在服务器的成绩, 仅学校有权限访问, 考评系统直接在封闭体系评分, 删除权限在学校手中;
- 5、仅院校指定的服务器可下载考试成绩, 下载到本地的成绩数据仅管理员有权限查看, 评分过程即可以完全使用考务系统封闭体系, 也可以在学校局域网环境进行, 评分过程产生的所有数据可以均在校本地, 防止外网攻击;
- 6、考务系统平台工作人员访问痕迹均有日志记录, 不可删除, 可有效追踪管理。

备注：考务系统打分比传统纸质打分更安全，一方面表现在打分过程加密处理，不可编辑修改；另一方面大大减少了后期成绩录入过程中的失误。同时考务系统提供了两城三地级别的数据异地容灾备份功能。容灾备份是实时及每日相结合，使用 VPN 专线连接了多个备份机房。

## （二）考生个人信息安全

- 1、学校导入到平台的数据，考务系统平台仅作为识别是本校已报名考生身份使用，院校端后台管理权限在院校手中；
- 2、考生注册认证过程存留在平台的数据，考生考试完成可随时注销账号，与该考生相关数据均自动删除；
- 3、考生考试结束后，考务系统平台可按照学校要求删除与学校直接关联的所有数据；
- 4、考务系统平台工作人员访问痕迹均有日志记录，不可删除，可有效追踪管理。

## （三）考务系统内部管理安全

- 1、考务系统工作人员均和公司签订有保密协议，确保员工对工作期间接触的核心数据保密；
- 2、考务系统公司内部可访问核心数据的权限十分严格，按照国家三级等保要求执行。
- 3、考务系统已获得国家三级等保认证和完成教育部移动应用备案

备注：国家等级保护认证是中国权威的信息产品安全等级资格认证，由公安机关依据国家信息安全保护条例及相关制度规定，按照管理规范和技术标准，对各机构的信息系统安全等级保护状况进行认可及评定。其中三级等保是国家对非银行机构的最高级认证，属于“监管级别”，由国家信息安全监管部门进行监督、检查，认证测评内容分别涵盖 5 个等级保护安全技术要求

和 5 个安全管理要求，包含信息保护、安全审计、通信保密等近 300 项要求，共涉及测评分类 73 类，要求十分严格。

#### （四）保密协议保障安全

- 1、考务系统根据和学校达成一致要求，签订保密协议；
- 2、考务系统与其他合作的国内顶尖高校，也是按照同样高标准执行保密协议，这些顶尖学府都是在国内有巨大影响力的高校。
- 3、考务系统服务于高考、研究生统考、成人高考、技能高考、艺术高考、体育高考等诸多最高等级的考试，提供全套考试信息系统。

#### （五）系统安全

1、 软件安全是指确保计算机软件的完整性以及不被破坏或是泄漏。软件的完整性指的是系统应用软件、数据库管理软件等相关资料的完整性，系统软件在保证网络系统正常运行中发挥着重要的作用。

##### 1.1 代码审查策略

1.1.1 所有已开发功能首先都在测试环境进行功能调试，调试通过后需提交至版本服务器进行代码审查，审查通过后方可编译发布至生产服务器。

1.1.2 所有已上线的功能，都保留一份已编译的代码和一份源代码，设计数据库结构改动的还会保留一份数据库结构备份文件。

1.1.3 APP 鉴权认证：业务访问服务需要通过 appid 和 appkey 才能接入服务。

1.1.4 客户端通讯安全：客户端与服务器的交互信令是在 ssl 基础上，对传输的数据做二次加密，使得链路上数据传输无法获取明文内容。

1.1.5 日志存储安全：客户端本地的日志加密，需要专属工具才能解析日志，避免关键流程和敏感信息通过日志泄漏。

1.1.6 业务安全：根据不同业务场景，设计不同技术流程，减少或避免在通

讯过程及无关逻辑上接触敏感业务数据，从源头杜绝安全隐患。

## 2、 系统软件安全措施

我们会定期检查系统软件，对系统软件进行有效管理，及时的发现安全隐患，针对存在

的问题来适当的改进现行的软件，以保证系统软件的安全。

在正式对系统软件进行加载之前，先检测系统软件，确定系统软件和其他应用软件之间

是否兼容，对检测结果的真实性、准确性负责，对检测软件的结果做完整的记录。

## 3、 软件安全措施

在计算机中安装两份软件，一份运行，一份备份，当运行的软件出现问题影响到系统的

正常运行时，就运行备份软件。比较这两个软件，如果备份软件也在运行中出现问题的，则说明该软件存在造成网络信息系统出现故障的隐患，面临着安全的威胁；如果备份软件在运行过程中是正常的，就将备份软件复制一份，再进行相同的检测。

## 4、 网络安全

网络的开放性带来了方便的可用性，但也使其更容易受到外界的攻击和威胁。入侵者可以利用系统中的安全漏洞，采用恶意程序来攻击网络，篡改、窃取网络信息，从而导致网络瘫痪、系统停止运行。在网络维护过程中，我们采用云盾、DDOS 等安全厂商多级防设备严格的与网络攻防行为对抗，保障网络安全。

### 4.1 网络结构安全保护措施

网络信息系统为了保证内部网络拓扑信息不被非法获得，在不对性能造成

影响的前提下，采用 VPN 虚拟专用网络并以多重身份认证系统隔离内部网络；在网络信息系统内部采用划分 VLAN 的方法来防止非法窃听；采取监控、隔离的措施来保护重要的服务器。

#### 4.2 网络系统设备安全保护措施

网络系统的网络设备配备防火墙、入侵检测系统、以及行为审计系统等。

4.2.1 防火墙：防火墙的抗攻击能力特别强，它是不同网络以及网络安全域信息交换的唯一出入口，功能包括：网络数据包过滤功能、访问控制功能、网络访问行为功能以及安全审计、安全告警功能；

4.2.2 入侵检测系统：入侵检测系统可以协助系统对付网络攻击，主动保护自己免受攻击，使信息安全基础的结构更加的完整。入侵检测系统功能包括：实时监测网络上的数据流，分析处理和过滤生成的审计数据；联动功能和自动响应功能是否正常；身份认识功能是否合理有效，什么权限的授权人员才有资格设置入侵管理规则，才能查阅、统计、管理以及维护日志记录，其他人不能任意的更改或删除日志记录；

4.2.3 病毒防范系统：病毒防范系统功能包括：病毒防范功能、病毒特征库更新功能以及审计数据生成与管理。病毒防范系统安全检测包括：能控制病毒侵入途径，控制并阻断病毒在系统内传播；系统能在病毒侵入时应及时的隔离、清除病毒，在日志上详细记录病毒时间的发生及处理过程；病毒特征库定期更新，定期统计和分析病毒的相关日志记录，及时的对病毒防范策略进行调整；

4.2.4 漏洞扫描仪：漏洞扫描仪会定期扫描系统，发现系统漏洞，防范于未然。系统漏洞信息具有双面性，维护人员尽早发现它可采取措施填补，不法分子也可利用它搞破坏。只有授权人员才能对漏洞扫描器进行查阅、管理、统计、维护扫描报告，只有授权人员才能制定扫描规则，定义攻击类型、标



准服务类型以及 IP 地址，授权使用者会定期更新扫描特征数据库，并及时的调整安全策略，更新反病毒数据库或设置更高的保护级别。

4.2.5 安全审计系统：审计数据是系统根据设置的审计规则产生的，审计系统功能包括：

审计查阅功能、选择性审计功能。只有授权人才有权查阅审计系统的日志记录；采取加密保护措施来确保日志的安全，任何人不得随意更改日志记录。

#### 4.3 网络系统可用性保护措施

网络系统的可用性是网络信息系统安全要求的重要组成部分，保证网络系统安全的技术

手段有：网络冗余、技术方案验证、网络管理和监控等方面。其中，网络冗余是解决网络故障的重要措施，备份重要的网络设备和网络线路，实时监控网络的运行状态，一旦网络出现故障或是信息流量突变可以及时的切换分配，确保网络的正常运行。我们适当的采用网络监控系统、网络管理系统这些网络管理和监控手段，运用网络故障发现、网络异常报警等功能来确保网络运行的安全。

#### 4.4 具体实施策略

4.4.1 服务器统一在认证机构采购或我公司自运营。对不同服务器进行业务隔离，为系统投产后能最大限度保证运行安全；

4.4.2 服务器的登录采用 VPN 虚拟专用网络并以多重身份认证系统隔离内部网络，在网络信息系统内部采用划分 VLAN 的方法来防止非法窃听，以保证链路安全；

4.4.3 服务器需采用严格的安全组策略，根据服务器的具体用途设立对应的安全策略，其中：

4.4.3.1 除 80/443 和 8080/8443 端口开放为公共端口外，其余一律端口按设置规则实际需要访问，优先级为较低；

4.4.3.2 远程登录端口须设为仅运维环境可访问，优先级为最高；

4.4.3.3 测试服务器仅开发环境可访问，以免与生产环境混淆；

4.4.3.4 如有与外部单位进行对接业务的，可根据实际开放相应端口和 IP 访问权限；

4.4.4 所有公共对外的服务器均一律接入第三方云盾或华为 NFW 下一代防火墙系统，并定期登录进行巡查和策略调整，并对安全监测进行危险性分级，实施 7\*24 小时不间断监控和报警；

4.4.5 所有服务器采用云监控服务，实现对主机的实时监控和防护；

4.4.6 生产服务器采用双机热备份策略，能在单机故障情况下实现自动切换。

#### 4.5 并发支撑

4.5.1 在可扩展性方面，系统通过多种不同策略来控制服务的水平扩展和平稳扩容，包括 http 类服务通过域名调度和负载均衡服务来进行处理，媒体服务通过调度中心的负载计算和就近接入的分组策略来实现节点的增加和删除，整个过程对用户透明。

4.5.2 在可用性方面，在可靠性设计的基础上，无单点，健康检查，自动重试，主备存储等机制，系统还实现以下设计来进一步确保可用性：

4.5.3 限流/切流量：当某应用流量忽然增大时，系统域名调度，负载均衡策略自动或者半自动切换应用流量；

4.5.4 无缝升级：系统所有服务的升级可以做到让线上用户基本无感知，或者通过 SDK 的自动重试策略恢复使用。

4.5.5 目前 考务系统经过多轮压力测试，至少可以支撑 650 万考生同时考试。

