政府采购合同（服务类）

合同编号：

项目编号：11000023Y000002159526

招标编号：BMCC-ZC24-0279/5

项目名称：信息系统运维类项目—应用平台运维与服务支撑

服务名称：北京市普通高中生综合素质评价电子平台运维

甲　方（买方）：北京市数字教育中心（北京电化教育馆）

乙　方（卖方）：沐华清诚（北京）教育科技发展有限公司

签署日期：2024 年 6 月 18 日

合　　同　　书

北京市数字教育中心（北京电化教育馆）（以下简称“甲方”）信息系统运维类项目—应用平台运维与服务支撑项目中所需北京市普通高中生综合素质评价电子平台运维以 BMCC-ZC24-0279/5 号招标文件在国内公开招标。经评标委员会评定沐华清诚（北京）教育科技发展有限公司 （以下简称“乙方”）为中标人。甲乙双方同意按照下面的条款和条件，签署本合同。

1、合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 中标通知书

c. 协议

d. 投标文件　　（含澄清文件）

e. 招标文件　　（含招标文件补充通知）

2、合同总价

本合同含税总价为人民币¥1139000.00 元。

人民币大写金额为： 壹佰壹拾叁万玖仟元整。

3、付款方式

合同签订后 10 个工作日内，乙方向甲方提交合同总额 10% 的履约保证金，计¥113900 元（大写：人民币壹拾壹万叁仟玖佰元整）；合同签订且收到发票后的 10 个工作日内甲方付合同总额的 40%给乙方，计¥455600.00 元（大写：人民币肆拾伍万伍仟陆佰元整）；2024 年 9 月 30 日前，乙方完成甲方指定的阶段性项目工作且未产生合同约定的违约行为，甲方在收到发票后的 10 个工作日内向乙方支付合同总价的 20%；计¥ 227800.00 元（大写：人民币贰拾贰万柒仟捌佰元整）；2024 年 11 月 30 日前，乙方完成甲方指定的阶段性项目工作且未产生合同约定的违约行为，甲方在收到发票后的 10

个工作日内向乙方支付合同总价的 10%，计¥113900.00 元（大写：人民币壹拾壹万叁仟玖佰元整）；2025 年 6 月 30 日前，乙方完成甲方指定的阶段性项目工作且未产生合同约定的违约行为，甲方在收到发票后的 10 个工作日内向乙方支付合同总价的 30%，计¥341700.00 元（大写：人民币叁拾肆万壹仟柒佰元整）；项目验收通过后，甲方无息退还乙方履约保证金。

4、本合同服务提供的内容、时间及交货地点

服务内容：见附件

执行地点：北京市数字教育中心指定地点

服务期：2024 年 8 月 18 日-2025 年 8 月 17 日

5、合同的生效。

本合同经双方授权代表签字、加盖单位印章后生效。

甲　方：北京市数字教育中心（北京电化教育馆）

名　称：（印章）

2024年6月18日

授权代表人（签字）：吴昊

地址：北京市西城区地安门西大街 153 号

邮政编码：100035

乙　方：沐华清诚（北京）教育科技发展有限公司

名　称：（印章）

2024年6月18日

授权代表人（签字）：张伟

地址：北京市海淀区双清路 77 号院 4 号楼 13 层 101

邮政编码：100085

附：中标通知书

1611-

中 标 通 知 书

项目名称：信息系统运维类项目—应用平台运维与服务支撑

项目编号：BMCC-ZC24-0279/5

01 包：

中标供应商：沐华清诚（北京）教育科技发展有限公司

中标金额：1,139,000.00 元

合同签订后 2 个工作日内，请将合同扫描件发送到 bjmdzx@vip.163.com 邮箱办理相关备案及保证金退还手续，保证金将在合同签订的 5 个工作日内退回来款账户。

邮件格式：项目编号+退还投标保证金+供应商名称+已签订采购合同。内附：（1）采购合同扫描件；（2）项目编号；（3）中标供应商名称；（4）采购合同签订日期。

北京明德致信咨询有限公司

2024 年 5 月 31 日

北京明德致信咨询有限公司

地址：北京市海淀区学院路 30 号科大天工大厦 B 座十七层 1709 室

电话：010-82370045　传真：010-82370045

邮箱：bjmdzx@vip.163.com

合 同 一 般 条 款

1、定义

本合同中的下列术语应解释为：

1.1 “合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和构成合同的其它文件。

1.2 “合同价”系指根据合同约定，乙方在完全履行合同义务后甲方应付给乙方的价格。

1.3 “服务”系指根据合同约定乙方提供的技术服务。

1.4 “甲方”系指与中标人签署供货合同的单位（含最终用户）。

1.5 “乙方”系指根据合同约定提供货物及相关服务的中标人。

1.6 “现场”系指合同约定的技术服务的地点。

1.7 “验收”系指合同双方依据强制性的国家技术质量规范和合同约定，确认合同项下的货物或服务符合合同规定的活动。

2 知识产权

2.1 乙方应保证甲方在使用该货物或服务或其任何一部分时不受第三方提出的侵犯专利权、著作权、商标权和工业设计权等的起诉。如果任何第三方提出侵权指控，乙方须与第三方交涉并单独承担由此发生的一切责任、费用和经济赔偿。

3 付款条件

合同签订后10个工作日内，乙方向甲方提交合同总额 10% 的履约保证金，计¥113900 元（大写：人民币壹拾壹万叁仟玖佰元整）；合同签订且收到发票后的10个工作日内甲方付合同总额的 40%给乙方，计¥455600.00 元（大写：人民币肆拾伍万伍仟陆佰元整）；2024年9月30日前，乙方完成甲方指定的阶段性项目工作且未产生合同约定的违约行为，甲方在收到发票后的10个工作日内向乙方支付合同总价的20%；计¥ 227800.00 元（大写：人民币贰拾贰万柒仟捌佰元整）；2024年11月30日前，乙方完成甲方指定的阶段性项目工作且未产生合同约定的违约行为，甲方在收到发票后的10个工作日内向乙方支付合同总价的10%，计¥113900.00 元（大写：人民币壹拾壹万叁仟玖佰元整 ）；2025年6月30日前，

乙方完成甲方指定的阶段性项目工作且未产生合同约定的违约行为，甲方在收到发票后的10个工作日内向乙方支付合同总价的 30% ，计¥341700.00元（大写：人民币叁拾肆万壹仟柒佰元整）；项目验收通过后，甲方无息退还乙方履约保证金。

4 交货

4.1 乙方在合同约定的服务期限内完成技术服务。

5 验收

5.1 甲方对乙方完成的技术服务，按照招标文件和投标文件的约定进行验收。

6 索赔

6.1 如果所提供的技术服务与和合同约定的不符，或存有缺陷，甲方有权向乙方提出索赔。

6.2 如果在甲方发出索赔通知后 10 个工作日内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方提出索赔通知后 10 个工作日内或甲方同意的更长时间内支付索赔款项，甲方将从合同款中扣回索赔金额。如果这些金额不足以补偿索赔金额，甲方有权向乙方提出不足部分的补偿。

7 延迟交货

7.1 乙方应在招标文件中规定的服务期限内提交技术服务。

7.2 如果乙方无正当理由迟延提交技术服务，甲方有权提出违约损失赔偿或解除合同。

7.3 在履行合同过程中，如果乙方遇到不能按时提交技术服务的情况，应及时以书面形式将不能按时交予的理由、预期延误时间通知甲方。甲方收到乙方通知后，认为其理由正当的，可酌情延长交货时间。

8 违约赔偿

8.1 除合同第 7 条规定外，如果乙方没有按照招标文件中规定的服务期限内提交技术服务，甲方可要求乙方支付违约金。违约金按每周合同价的 0.5%计收，但违约金的最高限额为合同价的 30%。一周按 7 天计算，

不足 7 天按一周计算。如果达到最高限额，甲方有权解除合同，并且乙方缴纳的履约保证金不予退还。

9 不可抗力

9.1 如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

9.2 受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后 7 天内，将有关部门出具的证明文件送达另一方。

9.3 不可抗力使合同的某些内容有变更必要的，双方应通过协商在 7-15 日内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

10 税费

10.1 与本合同有关的一切税费均适用中华人民共和国法律的相关规定。

11 合同争议的解决

11.1 因合同履行中发生的争议，合同当事人双方可通过协商解决。协商不成的，任何一方均可诉至甲方所在地的人民法院。

11.2 诉讼费、保全费、公证费、律师费等应由败诉方负担。

12 违约解除合同

12.1 在乙方违约的情况下，甲方可向乙方发出书面通知解除合同。同时保留向乙方追诉的权利。

12.1.1 乙方未能在合同规定的限期或甲方同意延长的限期内，提供全部或部分服务,按合同第 12.1 的规定可以解除合同的;

12.1.2 乙方未能履行合同规定的其它主要义务的;

12.1.3 在本合同履行过程中有腐败和欺诈行为的。

12.1.3.1 “腐败行为”和“欺诈行为”定义如下:

12.1.3.1.1 “腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响甲方在合同签订、履行过程中的行为。

12.1.3.1.2 “欺诈行为”是指为了影响合同签订、履行过程，以谎报事实

的方法，损害甲方的利益的行为。

12.2 在甲方根据上述第 12.1 条规定，合同解除后，尚未履行的，终止履行；已经履行的，根据履行情况和合同性质，甲方可以要求乙方恢复原状、采取其他补救措施，并有权要求赔偿损失。

13 破产终止合同

13.1 如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方，单方终止合同而不给乙方补偿。但甲方必须以书面形式告知同级政府采购监督管理部门。该合同的终止将不损害或不影响甲方已经采取或将要采取的任何行动或补救措施的权利。

14 转让和分包

14.1 政府采购合同不能转让。

14.2 经甲方书面同意，乙方可以将合同项下非主体、非关键性工作分包给他人完成。接受分包的人应当具备相应的资格条件，并不得再次分包。分包后不能免除乙方履行本合同的责任和义务，乙方与接受分包的主体共同对甲方连带承担合同的责任和义务。乙方可以将合同项下非主体、非关键性工作分包给他人完成。但必须在投标文件中载明。

15 合同修改

15.1 甲方和乙方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，当事人双方须共同签署书面文件，作为合同的补充。

16 通知

16.1 本合同任何一方给另一方的通知，都应以书面形式发送，而另一方也应以书面形式确认并发送到对方明确的地址。

17 计量单位

17.1 除技术规范中另有规定外，计量单位均使用国家法定计量单位。

18 适用法律

18.1 本合同应按照中华人民共和国的法律进行解释。

19 履约保证金

19.1 合同签订后 10 个工作日内，乙方向甲方提交合同总额的 10% 履约保证金。

19.2 履约保证金用于补偿甲方因乙方不能履行其合同义务而蒙受的损失。在乙方出现违约情形时，甲方有权不予退还履约保证金，并有权按照合同约定向乙方主张违约责任。

19.3 履约保证金应使用本合同货币，按下述方式之一提交：_____

A. 金融机构、担保机构出具的保函等非现金形式提交。

B. 支票、汇票、本票、转账。

19.4 履约保证金在法定的服务质量保证期期满前应完全有效。如果乙方未能按合同规定履行其义务，甲方有权从履约保证金中取得补偿。

19.5 履约保证金将于项目验收通过后无息返还。

20 合同生效和其它

20.1 政府采购项目的采购合同内容的确定应以招标文件和投标文件为基础，不得违背其实质性内容。本合同经双方授权代表签字、加盖单位印章后生效。

20.2 本合同一式 5 份，以中文书写，甲方 3 份，乙方 2 份。

附件：服务内容

一、本项目的运维服务方案

（一）本项目的运维服务承诺

致：北京市数字教育中心（北京电化教育馆）

就信息系统运维类项目—应用平台运维与服务支撑（01-北京市普通高中生综合素质评价电子平台运维）的服务要求，我司承诺如下：

1、 我司提供服务周期为2024年8月18日至2025年8月17日。

2、 针对北京市普通高中生综合素质评价电子平台运维服务，我司承诺提供培训与用户反馈收集服务、技术运维服务、特殊时期保驾运维服务，服务内容满足采购需求。

3、 我司作为北京的本地企业，可利用本地便利优势，提升服务相应速度，

扩大服务对象范围，深入了解学校开展综评工作遇到的问题，帮助当地学校提高素质教育和综合素质评价工作水平。我司承诺当接到用户问题反馈时，30分钟内响应，远程服务无法解决问题的，2小时内技术工程师到达市、区级教委或学校帮助解决问题。

4、 我司承诺满足采购需求中要求的其他需求。

投标人： 沐华清诚（北京）教育科技发展有限公司

公章：

日期：2024年05月27日

（二）用户反馈收集服务

1、用户反馈收集方式

日常我司通过QQ群（群号715054727）答疑、客服电话（电话010-82567914）接听、系统培训、薄弱学校指导等服务过程中收集用户反馈。

2、用户反馈收集

汇总各方面反馈得来的意见，进行整理分析。

3、用户反馈处理

针对用户反馈内容，依据现有安全、成熟的技术路线，制定相应的解决方案。用户反馈内容主要包含系统操作问题、系统功能需求、政协相关问题等三类，具体处理方案如下：

1）系统操作问题。

针对系统操作问题，服务团队通过QQ群、客服电话等远程方式及时响应，解答相关操作问题，对于普常见操作问题更新《用户常见问题》操作提示文件。

2）政策相关问题

针对政策问题，服务团队定期整理汇总，反馈至教委，根据教委意见处理。

3）系统功能需求

定期对系统功能需求进行整理分类、分析：

①功能优化需求：针对必要需求进行系统原有的功能优化，确保区教委的管理员、校管理员、老师和学生都能够切实的把系统用好。

②针对定制需求：

依据现有安全、成熟的技术路线，制定相应的解决方案呈报北京市教委审核，教委审核通过后，按照方案计划逐步实施；如果审核不通过，根据北京市教委的意见改进解决方案，待审核通过之后，解决用户需求。功能开发完成上线之后，对用户进行回访，确保用户需求得以满足。

4、计划安排

在本项目运维服务期间，我司将组织6次用户反馈收集会服务。

（三）薄弱学校指导服务

1、工作内容

（1）综评工作薄弱校选择

由教委负责遴选薄弱学校，形成薄弱学校指导名单，服务团队根据名单分批开展薄弱学校指导服务。

（2）组织方式

薄弱学校指导服务可根据学校实际情况采用线上或线下会议的方式进行。

（3）服务时间

根据教委确定的薄弱学校指导名单，分别与学校沟通，确定服务时间，对接人，组织方式、服务内容，学校参与人员，为指导学校做好准备。

（4）服务指导

在商定的时间内，服务团队与学校相关负责人（如综评负责人、教师代表、管理员代表、学生代表等）一起，通过线上或线下的方式进行沟通，听取学校在使用过程中面临的困难，并进行分析解答。对于系统操作问题现场解答，对于政策问题进行记录及反馈至教委，对于功能需求进行记录和分析，必要的功能完成优化。如果需要，还可以组织一场小型的培训会。

2、工作安排

服务团队根据教委的薄弱学校指导名单分批开展薄弱学校指导服务。

服务项目	计划安排
薄弱学校指导服务	2024 年 10 月开展薄弱学校指导服务一次
	2024 年 11 月开展薄弱学校指导服务两次
	2024 年 12 月开展薄弱学校指导服务一次
	2025 年 3 月开展薄弱学校指导服务一次
	2025 年 4 月开展薄弱学校指导服务一次

注：此工作安排为预案，实施过程中将根据北京市实际情况进行调整。

（四）特殊时期运维服务

北京市将作为第二批高考改革试点城市，在新高考改革政策下，2020年开始学生的综合素质评价结果已作为高考录取的参考。为保证2025年度高中工作顺利进行，为此，我司将从2025年3月至6月提供特殊时期运维服务，为北京市教委、高招单位提供及时、准确、有效的综合素质评价数据。工作内容如下：

（1）强基计划服务

2025年3月、4月，服务团队针对2025届高中毕业生提供强基计划材料处理服务，服务包括协助北京市教委完成毕业生名单导入、材料校核、合规材料分组、

不合规材料剔除和说明、根据强基计划要求生成报告册及报送等。

（2）提前批学生数据处理

在高考前期，针对高校提前招生等情况，服务团队提供提前批学生数据处理服务。服务内容包含综评数据提前处理及报告册生成等。

（3）学籍异常处理

在报告册生成阶段，服务团队针对少年班、提前报考、复学、往届生等学籍异常学生提供综评数据处理服务及报告册生成等服务。

（4）数据查询服务

根据预案对于数据查询的流程设定，指派专门的数据服务小组，根据教委各级审定的查询服务要求，为高招部门提供数据查询服务，并把查询结果发送给高招部门。

由技术工程师1人和数据工程师1人组成一组为招生部门提供查询服务。其中技术工程师负责与高招的老师沟通确认数据需求，并根据需求确定查询方案。数据工程师负责数据查询，检查，由技术工程师负责呈报。

根据毕业生数量预判，预计需要4组工程师提供服务2周，合计4人月，可完成近6000余人次检索，约占毕业生数量的10%。

（5）其他高招所需数据服务

高校招生过程中，有可能对提档线的学生进行排序、标签筛选等数据服务，为此我司提供2组工程师（技术工程师1人，数据工程师1人）提供数据应用服务2周，合计1人月。可提供近2000次服务，可满足高校招生要求。

（6）报告册填报进度监督

我司在特殊时期对学生报告册填报进度进行监控，可根据教委需求提供各区的填报进度情况。

（五）技术运维服务

1、应用系统运行监控

应用系统运行监控我司采用zabbix和shell脚本监控的双监控体系，能有效的对服务器CPU负载、服务器1分钟、5分钟、15分钟的平均负载、内存使用率、磁盘使用率、应用服务和系统服务端口进行有效监控。在系统或服务状态异常时发出邮件或企业微信报警第一时间通知网站运维人员，及时处理问题，保证系统

正常运行。

使用zabbix和shell脚本监控对综评系统进行监控，其功能特性介绍如下：

（1）综合资源监控，不遗漏任何死角

网络监控：全面监控内网网络丢包率等信息。

主机监控：涉及到CPU、内存、硬盘等各个方面。

应用监控：支持几乎所有主流应用系统的监控，包括：数据库、Web服务。

存储监控：监控各种不同存储设备可用性和使用率等信息。

基础业务监控：在后台各项监控的同时注重业务表现的直观监控，比如业务应用的访问页面URL、业务应用端口等内容，给管理员最直观的业务影响判断。

（2）实时性能分析，增强监控可靠性

主机实时分析：对选定主机的CPU使用率、内存使用率等性能指标进行实时分析，间隔周期最小可设定为5秒。

应用实时分析：对选定应用系统的关键性能指标进行实时分析，按照各种应用系统的侧重点不同提取系统级重点指标进行高密集度的实时性能展现。

（3）报警机制

在系统或服务状态异常时，3分钟内发出邮件或企业微信报警，第一时间通知网站运维人员，及时处理问题，保证系统正常运行。

邮件报警：当出现故障时采用邮件方式通知管理员。

企业微信报警：当出现故障时采用企业微信形式的方式通知管理员。

系统监控体系一般部署在资源中心的内网服务器上，内网服务器根据网络安全策略不能对外发起网络访问，为此，我司单独开发一个服务，部署在应用服务器上，每当出现预警报警信息时，由我司监控中心每三分钟调用该服务，保证在3分钟内产生的预警报警信息可以及时的获取到，并以邮件和微信的方式通知管理员。在保证网络安全的基础上，实现了预警报警信息快速传递，可以极大的提升系统运行安全保障能力。

告警指标	性能告警阀值	机制
数据库服务CPU使用率	＞30%	发出报警
应用服务CPU使用率	＞70%	发出报警
数据存储使用率	＞60%	发出预警

	＞80%	发出报警
服务可用情况	服务接口访问反应时间大于5秒的数量＞500次/3分钟	发出报警

2、基础维护服务

（1）系统巡检

以自然月为单位，开展定期巡检服务。巡检服务主要工作是根据日常总结的运行模式，比对当前运行的各种指标参数及日志情况，定位当前系统的健康状况。在运行过程中指标越界予以关注，判断是否会产生影响系统服务的可能。在发现隐患的时候，尽快处理，防患于未然。巡检维度如下：

对系统巡检的评估维度主要包括以下六个方面：

1）应用服务器

①CPU使用是否正常

②内存使用是否正常

③盘空间是否足够

④是否有异常进程

⑤是否感染病毒

⑥是否升级最新系统补丁

2）负载均衡

①配置的各节点状态是否正常

②各节点的连接数是否正常

3）数据库

①表空间是否正常

②查看日志是否正常

4）Web服务器软件

①Nginx运行状态是否正常

②Nginx日志是否正常

5）数据备份

①备份脚本运行状况是否正常

②检查备份数据是否与线上一致

6）网站应用

①网站各功能是否正常

②网站点击量是否正常

③网站访问速度是否正常

（2）相关软件系统升级

对系统相关软件提供升级服务，以改进、完善现有系统或消除现有系统的漏洞。升级软件包含Web服务运行环境相关软件，数据库系统软件版本升级，数据库可视化软件工具，Linux系统组件，安全防护软件。

（3）数据库备份

数据库备份是确保数据完整性和可用性的关键过程，系统备份策略为全量备份。数据库备份工作包括应用系统备份与恢复、数据库备份。数据备份工作方式如下：

1）应用系统备份

程序和配置文件在做调整之前做备份，按照当天时间备份。

2）数据库系统备份

每天凌晨全量备份数据，备份数据最少保存最近15天的数据，最大保存180天的数据。

3）确认备份文件

次日上午检查备份文件是否生成。

（4）服务器性能优化

提供服务器性能优化服务，以提高服务器整体性能。服务器性能优化包括整体CPU性能瓶颈、内存性能瓶颈、磁盘I/O可调性能、网络可调性能等。

（5）补丁服务

提供软件补丁服务，定期关注相关软件更新补丁，及时了解可用补丁，完成补丁安装以消除软件漏洞及安全隐患，并对安装补丁所引起的系统连锁反应进行合理的平衡。

3、数据库维护

（1）数据库参数调整及性能优化

1）使用Linux性能命令free、top、iostat、iotop、strace 、tcpdump调优

2）调整MySQL缓存大小

3）优化数据库慢语句、MySQL服务器记录慢查询的阈值时间

4）优化binlog日志

（2）数据库监控

数据库端口监控、磁盘、内存、CPU监控。

（3）慢日志监控

慢日志监控是一种用于监控数据库中慢查询的方法，可以帮助识别和优化执行时间较长的查询，提高数据库的性能。

4、中间件维护

负责对Tomcat、Nginx等中间件的日常维护管理和监控工作，确保中间件平台保持持续稳定运行。具体工作包含中间件运行监控、中间件参数调整。

5、系统安全维护

（1）口令管理

1）强密码策略

密码复杂度：要求设置复杂的密码，包括大小写字母、数字和特殊字符。

密码更新频率：建议定期要求用户更改密码，例如每90天一次。

禁止常见密码：禁止使用常见的弱密码，如"123456"、"password"等。

禁止使用重复密码：禁止重复使用之前设置的密码。

2）口令访问控制

最小权限原则：为每个用户分配最小必要权限，避免赋予过高的权限。

口令策略检查：定期检查用户口令策略的合规性，确保遵守密码安全规定。

（2）排除安全隐患：

1）定期检查系统上是否存在异常进程

2）禁止给文件授权 777权限，权限开放到最小

3）敏感端口禁止对外开放

4）不使用弱口令或者空口令

5）验证对系统设置，程序文件和配置文件的更改

6）检查服务器以查找恶意软件和 rootkit

7）查找过期的用户帐户或未取消的管理员权限

6、故障诊断及处理

系统故障应急响应：7×24小时服务，重要节点增加人手重点保障；

系统故障诊断：在系统故障或者系统性能出现问题时，分别从业务系统，平台系统和数据库系统三个层面进行诊断。对业务系统日志，平台系统日志和数据库日志进行分析，找到故障原因，并确定解决方案。

故障处理：根据故障诊断结论，本着尽快恢复系统的原则，可以进行两级处理。第一级处理为系统恢复，让系统坚持运行，尽量减少系统服务中断时间。与此同时，制定完备的故障解决方案。在条件充分的情况下，一举解决故障。

通过两级处理的机制，可以减少系统故障或性能问题带来的系统服务中断时长，让综评系统的用户有好的体验。并且在二级处理后，系统的故障将得到彻底解决，不留后患。

（六）技术服务支持服务

我司开通热线电话和在线服务，通过电话、QQ、微信、Email等方式，解答用户的业务和技术咨询，为用户操作提供指引，处理系统的突发和异常情况等。

1、QQ群问题响应

综评系统公告管理与通知。在5×9小时由专人负责接收QQ群问题反馈并记录。根据问题情况时时做出解答。QQ群号715054727。

2、客服电话接听

在5×9小时由专人负责接听记录学校、师生、家长来电问题。对系统问题进行反馈，解答并记录。客服电话：010-82567914。

3、系统问题的收集整理、分析及反馈

针对各校及管理员使用情况，对反馈的问题进行收集整理，对于操作问题当场逐一反馈；政策问题反馈至教委；对于普遍的需求，由产品和技术部进行需求分解、分析，完成相应功能的优化。

（七）开发工程师服务

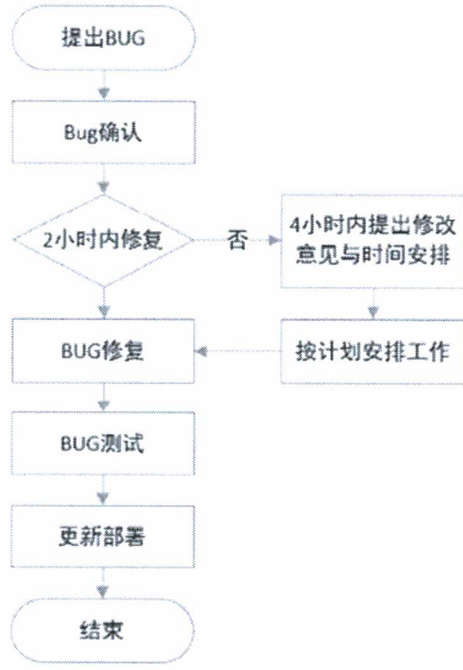
服务期内我司提供开发工程师服务，服务内容包含BUG和缺陷修复、系统功能优化。

1、BUG和缺陷修复

在应用系统维护期间，对于用户或维护工程师发现的系统BUG或者影响系统

正常运行的缺陷，我司提供BUG和缺陷的修复服务，及时修复BUG和缺陷，保障系统稳定运行和业务的正常开展。

当用户在使用过程中发现系统存在的问题时，开发工程师首先进行问题确认工作，确认是系统问题后，开始问题修复，如果不能在2小时内完成修复工作，在4小时内给出问题修改意见与实践安排，随后依次进行问题的修复、测试与部署工作。系统BUG和缺陷修复流程如下：

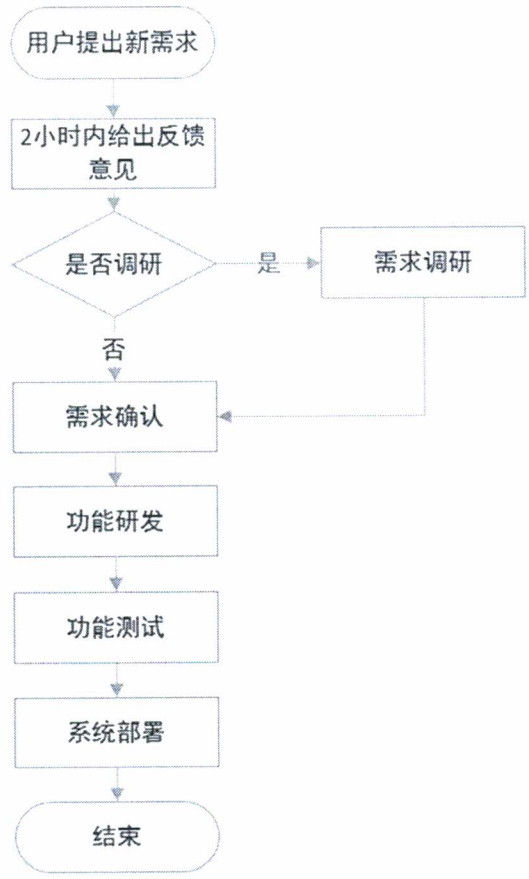


2、系统功能优化

在应用系统维护期间，由于客户业务发生变化从而需要对应用系统的相关功能模块进行升级改造。改造需求由用户提出，系统平台提供单位项目组团队进行需求分析、系统设计、编码、测试、上线一系列工作。

当用户提出新需求的时候，产品工程师在2个小时内给出意见，根据意见决定是否需要进行需求调研；如需要，进行需求调研工作；如不需要需求调研，则直接进入需求确认阶段；完成需求确认之后，开发工程师开始进行新功能研发工作，最后依次进行新功能的测试和部署工作。完成之后，由售后服务人员进行新功能使用的意见反馈等工作，进入售后服务流程。

具体流程如下：



（八）质量管理服务

质量管理是实现交付标准化管理的重要环节，通过多年的管理实践，结合业界的优秀管理模式，沐华清诚服务团队建立了完善的质量管理制度，确保项目能够按照服务标准进行执行，并达到客户的预期目标。针对本项目制定质量保障措施如下：

1、我司通过了ISO9001质量管理体系认证，将严格依照ISO9001标准执行本项目，确保质量管理体系的有效运行。

2、项目团队及人员能力

针对项目组建项目服务团队，按项目运维服务要求，分解运维服务内容，明确各服务团队成员责任及分工，确保每一项工作均有负责人。我司将对运维服务人员的知识、技能、经验、安全意识等方面进行评估和提升，确保其具备应有的能力和水平。

3、实施计划制定

项目实施前，根据运维服务要求制定详细的实施计划，明确项目的目标、时间计划和责任人。

4、项目进度跟踪

项目服务团队内部每周召开一次例会，由项目经理主持，各组负责人汇报施工进展，各组负责人并以月为单位将本月所完成工作以《项目月报》的形式提交给项目经理，由项目经理提交用户，帮助用户及时了解项目服务进度；

5、项目资料管理

在项目实施过程中，每个关键环节结束后，各组负责人将项目执行过程中产生的文件资料整理后提交给项目经理，由项目经理归档管理，作为各项服务完成的证明文件。

6、风险控制与管理

在项目实施过程中，风险是无法避免的，通过风险的预测、评估和控制，有效降低风险对项目的影响，从而确保项目目标的实现。

（九）应急处理服务

我司将针对本项目制定详尽的设计、实施方案，整个流程严谨而有序。但是，在整个项目实施过程中，意外情况将不可避免。下面，我们将对项目实施的突发风险进行详细分析，并且针对各类突发事件，设计了相应的预防与解决措施，同时提供了完整的应急处理流程。

我司将建立系统宕机、网络受限等各类故障问题应急处理机制，明确各类故障的应急预案及处理时效，至少在48小时内处理故障并做好应急响应。

1、应急处理机制和处理时效

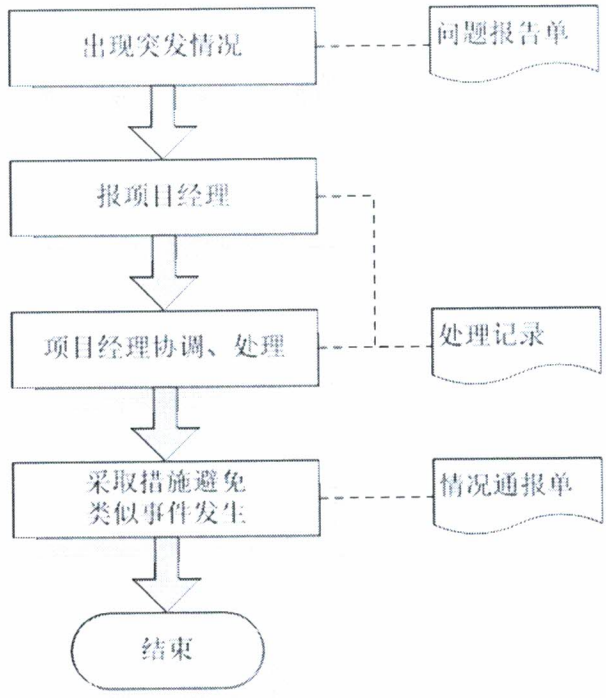
（1）应急处理原则

a、保护客户、员工、公司的利益。

b、统一领导、分级负责。

c、预防为主、随机演练。

（2）应急处理流程



2、应急报告管理

（1）内部报告要求

项目组内各岗位人员认真执行报告制度，做到事前请示，事后报告，确保工作对重大工作进展情况做到心中有数。实行逐级报告制度。凡属职责范围内的工作，要各负其责，认真落实。对于重大问题本级无法决定或处理，必须逐级上报，不得自作主张延误问题处理时间。

（2）外部报告要求

本着以客户至上的原则与客户进行沟通，内容必须充分翔实。

必须以书面（邮件）形式进行沟通报告，必要时可采用电话形式口头沟通，再进行邮件确认。

发生重大事项或突发事件时，如涉及生产或客户应第一时间与客户沟通解决，并上报主管领导。

3、应急报告处理

（1）为保证运营安全，在出现紧急事件时，项目经理应在第一时间向客户与我司高级运营管理人员就问题进行报告。

（2）建立应急联络表，给出我方必要联络人姓名、职务、联系方式、第二联系人与联系方式。

（3）建立常见应急事件处理预案及细则。

（4）各岗位负责人接到应急事件报告后，按照预案与细则，根据岗位分工进行组织、处置等工作。

（5）事件处理完毕后，由运营经理填写《紧急事件处置报告单》，对事件的响应及处理情况进行回顾、总结。此报告在事件发生三个工作日内应提交给我司运营总监。

附：　　紧急事件情况记录

事件发生时间		发生地点	
事件报告人		报告时间	
所在部门		项目负责人	
记录人		事件关闭时间	
突发事件说明			
处理过程描述	可描述谁发现，向谁报告等处理过程		
原因调查及 整改意见			
备注			

4、应急方案

（1）应急处理人员组织机构

应急机构人员岗位职责：

1）应急总指挥职责：

保证在任何时间，及时协调应急行动所有涉及的岗位人员；在紧急情况下全面负责紧急行动。

2）各相关负责人职责：

负责尽快收集信息向应急总指挥汇报事故情况；负责现场临时对事态的控制；听从上级指挥人员的指挥。

5、信息与网络安全突发事件处理原则

预防为主。立足安全防护，加强预警，重点保护基础信息网络和关系信息安全、稳定的重要信息系统，从预防、监控、应急处理、应急保障等环节，在管理、技术、人员等方面采取多种措施充分发挥各方面的作用，共同构筑信息与网络安全保障体系。

快速反应。突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

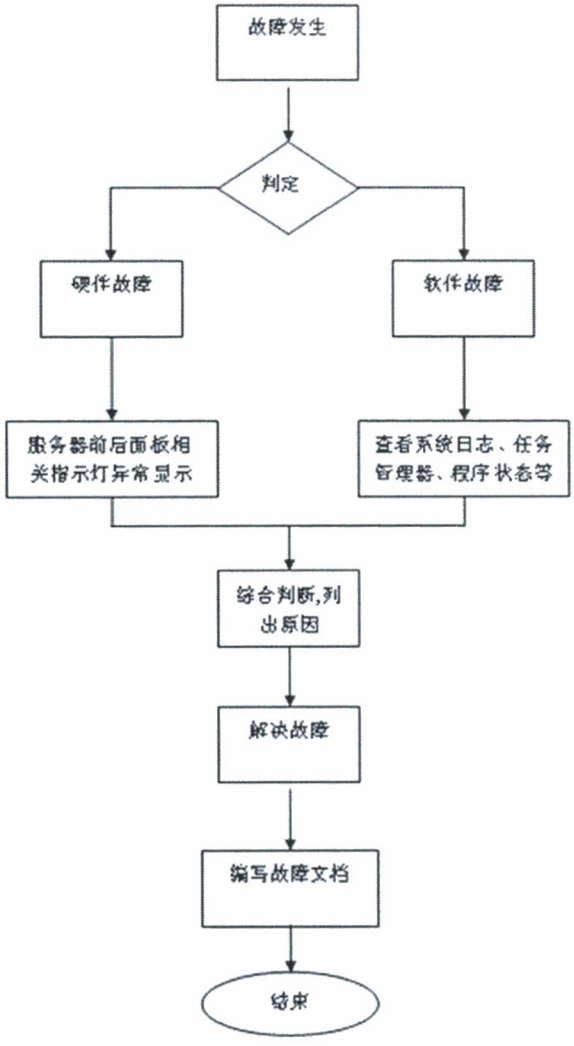
分级负责。按照“谁主管，谁负责”的原则，建立和完善安全责任制及联动工作机制。根据各负责人的职能，各司其职，加强各负责人的协调与配合，共同履行应急处置工作的管理职责。

以人为本。把保障人员以及公共利益的安全作为首要任务。

常备不懈。加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发公共事件应急处置的科学化、程序化与规范化。

6、服务支撑系统应急预案

（1）服务器突发情况应急预案



服务器设备损坏应急处置措施：

A、关键应用系统所在服务器设备损坏后，应立即查明原因，使用备份服务器替换损坏设备，并立即恢复应用系统正常使用;

B、立即与设备提供商联系请求派维修人员前来维修。

服务器软件损坏紧急处置措施：

A、迅速查找原因，尝试重启系统。使用备份进行恢复。必要时联系开发商;

B、当发现服务器感染有病毒后，应立即将该机从网络上隔离出来。并启用杀病毒软件对该机进行杀毒处理，同时使用病毒检测软件对其他机器进行病毒扫描和清除工作。经技术人员确认确实无法查杀该病毒后，应作好相关记录，并迅速联系有关产品商研究解决;

C、当因电力等问题需要关闭所有服务器时，应遵循如下步骤：

先关闭所有应用服务器和数据库服务器，再关闭存储设备。启动所有服 务

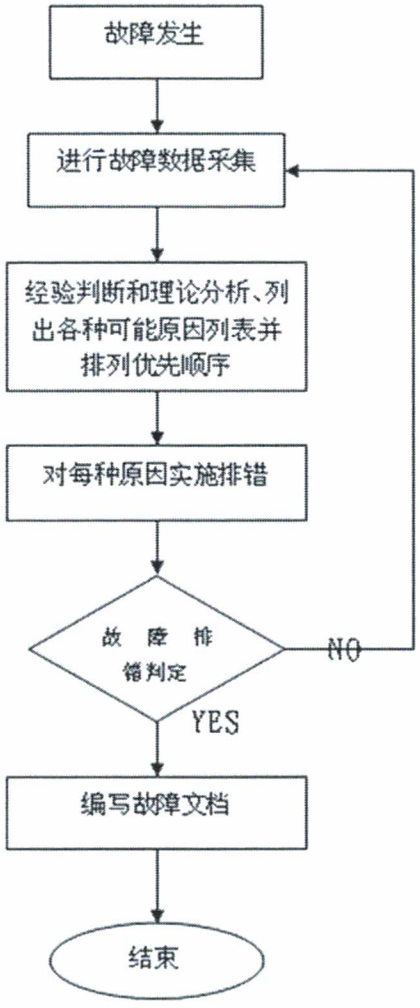
器时，应先打开存储设备，再打开数据库服务器，最后打开应用服务器。

服务器突发情况记录文档

日期	故障发生时间	服务器名称	IP	现象	处理情况	故障恢复时间	处理工程师	备注

（2）网络设备故障处理

下面流程图是网络维护人员所应采取的排错模型，当发生网络故障时应按照此流程快速进行定位、排除故障。



网络系统故障突发事件分级情况见下表：

故障等级	故障现象
1 级	网络完全拥塞或设备宕机

	网络或设备处理能力严重受影响，对最终客户的业务运作有严重影响
	网络或设备故障对重要的客户（公司经理级或重要的部门）造成严重影响
2级	网络或设备的性能严重下降，对最终客户的业务运作产生重要影响
	部分区域网络故障
	一般网络节点发生故障
	大部分客户的网络通讯质量下降
3级	网络或设备性能受损，但最终客户大部分业务仍可正常工作
	报警出错和操作命令反常
4级	其它一般的故障，不影响系统的整体运行，不影响大部分客户的使用

黑客攻击时的紧急处置措施

A、当发现网页内容被篡改、Internet接入路由器有未知用户登录或通过其他方式发现有黑客正在进行攻击时，应立即向信息部相关人员通报情况；

B、在信息部人员授权下，立即备份当时的log日志并采用端口限制方式阻断外部的入侵，观察被攻击的服务器等设备状态，同时向信息部领导汇报情况；

C、协调相关应用部门，与信息部有关技术人员一同负责被破坏系统的恢复与重建工作；

D、协助信息部人员协同有关部门共同追查非法信息来源；

E、情况严重的，根据突发事件级别应及时向有关上级部门汇报。

病毒安全紧急处置措施

A、当发现计算机感染有病毒后，应立即将该机从网络上隔离出来；或从网络设备状态发现病毒爆发应采取show mac-address sh arp定位或IP查询将病毒机器所在的网络设备端口shutdown；

B、通知维护人员对该设备的硬盘进行数据备份；

C、启用杀病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作；

D、如发现杀病毒软件无法清除该病毒，应立即通知用户并向及信息部负责人报告，经信息部技术人员确认无法查杀该病毒并同意格式化硬盘后，作好相关记录，并格式化硬盘；

E、机器恢复后重新开启网络设备的相应端口；

F、认为情况极为严重，根据突发事件级别应及时向有关上级部门汇报。

广域网线路中断紧急处置措施：

A、链路出现问题后，网络负责人切换至备用线路，应立即应急小组组长报告，沟通地方节点技术人员共同迅速判断故障，查明故障原因；

B、如属我方管辖范围，由双方技术人员立即配合予以恢复。如遇无法恢复情况，立即进行备件更换或向有关厂商请求支援；

C、如属运营商管辖范围，立即与运营商维护部门申报故障，请求修复；

D、根据突发事件级别应及时向有关上级部门汇报。

局域网中断紧急处置措施

A、局域网中断后，网络维护人员应立即判断故障节点，查明故障原因，并向信息部领导汇报；

B、如属线路故障，更换新线路或重新安装线路；或从最近飞线至故障设备；

C、如属路由器、交换机等网络设备（光模块）故障，应立即查找是否有相关备件可以替换，或与设备提供商联系更换设备，并调试畅通；

D、如属路由器、交换机配置文件破坏，应迅速按照备份配置文件重新配置，并调试畅通；如遇无法解决的技术问题，立即向有关厂商请求支援；

E、情况严重的，根据突发事件级别应及时向有关上级部门汇报。

网络突发事件记录文档：

日期	故障发生时间	线路	设备IP	端口	现象	处理情况	故障恢复时间	处理工程师	备注

（十）信息安全管控服务

我公司在长期与客户合作的过程中，深知信息安全是客户的业务保障，通过多年的运营管理经验，我公司在信息安全各方面均有完善的识别、预防（演习）、控制、审核、应对机制。

根据本项目的服务情况，我们主要对场地、设备、人员、数据等四个方面的信息安全进行管理。具体如下：

1、数据安全保护标准规范

（1）我司建立了完善的数据管理机制，对项目过程中所涉及数据信息的使

用、采集、存储等进行整体统一管控。

（2）本项目所使用的网络无路径、权限登陆外网，无法使用网络硬盘、网络空间、Internet邮箱免费邮箱传输任何数据。

（3）凡涉及到数据传输文件均设置用户要求的密码。

（4）计算机操作人员不得擅自让无关人员阅读计算机内贮存的工作信息。

（5）各类设备、信息、软件或纸制文档在未经授权情况下不得带离作业场所。

（6）计算机操作人员不得越权运行、查阅与自己工作无关的程序及数据。

（7）我方只存储、处理、传输双方约定的相关信息。

（8）我方确保所有可执行数据处理的人员都为得到有效授权的人员。

（9）我方确保相关数据访问权限得到最小化控制。

（10）任何人员不得私自记录客户个人信息、用户管理及业务要求。

2、技术监控

（1）系统采用独立的数据传输网络，防止恶意窃取，系统网络如需与外部网络连接，通过防火墙进行访问控制，阻止非法请求。

（2）采用双链路保障机制，当一条链路或者出口设备失效，还有另一条链路保证业务的可用性，保证接入链路的安全，确保业务的安全可靠。

（3）通过网络一体化设计和实施思想，保证核心骨干、边缘接入等多个部分网络的访问高安全性。

（4）建立统一的访问控制机制，服务(器)之间的网络访问均通过防火墙的源地址、源端口、目标地址、目标端口进行访问控制，在确保访问的合法性和有效性的前提下实现业务的安全运行。

（5）所有网络及安全设备以最小权限策略为基础，申请审批后方可打开相应端口和访问策略。

（6）所有网络及安全设备都进行了必要升级，升级软件的版本为相对稳定的版本，修补了重要安全漏洞。

（7）所有网络及安全设备关闭不需要开启的服务和协议，避免服务及协议的漏洞来降低网络安全。

（8）防火墙主要安全功能是在内部、外部两个网络之间建立一个安全控制

点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

（9）防火墙安全策略中默认策略和端口全部关闭，须按照要求开启。也就是说，除遵循防火墙的基本安全要求的访问（高安全级别可以访问低安全级别端口，低安全级别端口不能访问高安全级别端口），其他访问都是禁止状态。

（10）通过对网络及安全设备添加访问控制列表来避免授权用户访问非授权设备、端口等或非授权用户访问等现象的发生。

3、日常管理

（1）与其所有可能接触或知悉本项目任何秘密信息的人员签署保密协议。

（2）系统规划中如可能影响到处理用户信息的系统或网络，必须提前告知用户并取得书面同意。

（3）采用WORM（一次写多次读）机制记录日志，确保日志不可删除或修改；操作系统日志、网络通讯类日志以及应用类日志保存期限不少于三个月，数据库日志保存期限不少于一年。

4、系统的开发与维护

（1）系统开发与维护人员完全进行人员分离。

（2）开发、测试及生产系统进行隔离。

（3）不在测试环境中使用生产环境的数据，所有测试数据必须实行严格的保护，并且只能由甲方人员掌握，软件开发人员或我方人员若需接触必须先告知用户并得到用户书面的许可。如果需要在测试环境中使用生产环境的数据，需经用户书面许可并由用户人员监控使用过程。

（4）我方制定变更管理规定，并保证任何涉及用户的变更都须先告知用户并得到用户的书面许可下才可进行。

二、验收要求

1、履约验收内容：按照合同约定内容进行验收，按甲方规定的验收清单内容提供完整、规范的验收项目文档。

2、履约验收标准：本项目验收于完成合同约定的服务内容结束后进行，由北京市数字教育中心组织专家验收会进行项目验收，实施方应完成全部服务内容，并且提供相关的服务过程文档材料，证明项目质量要求达到优良。