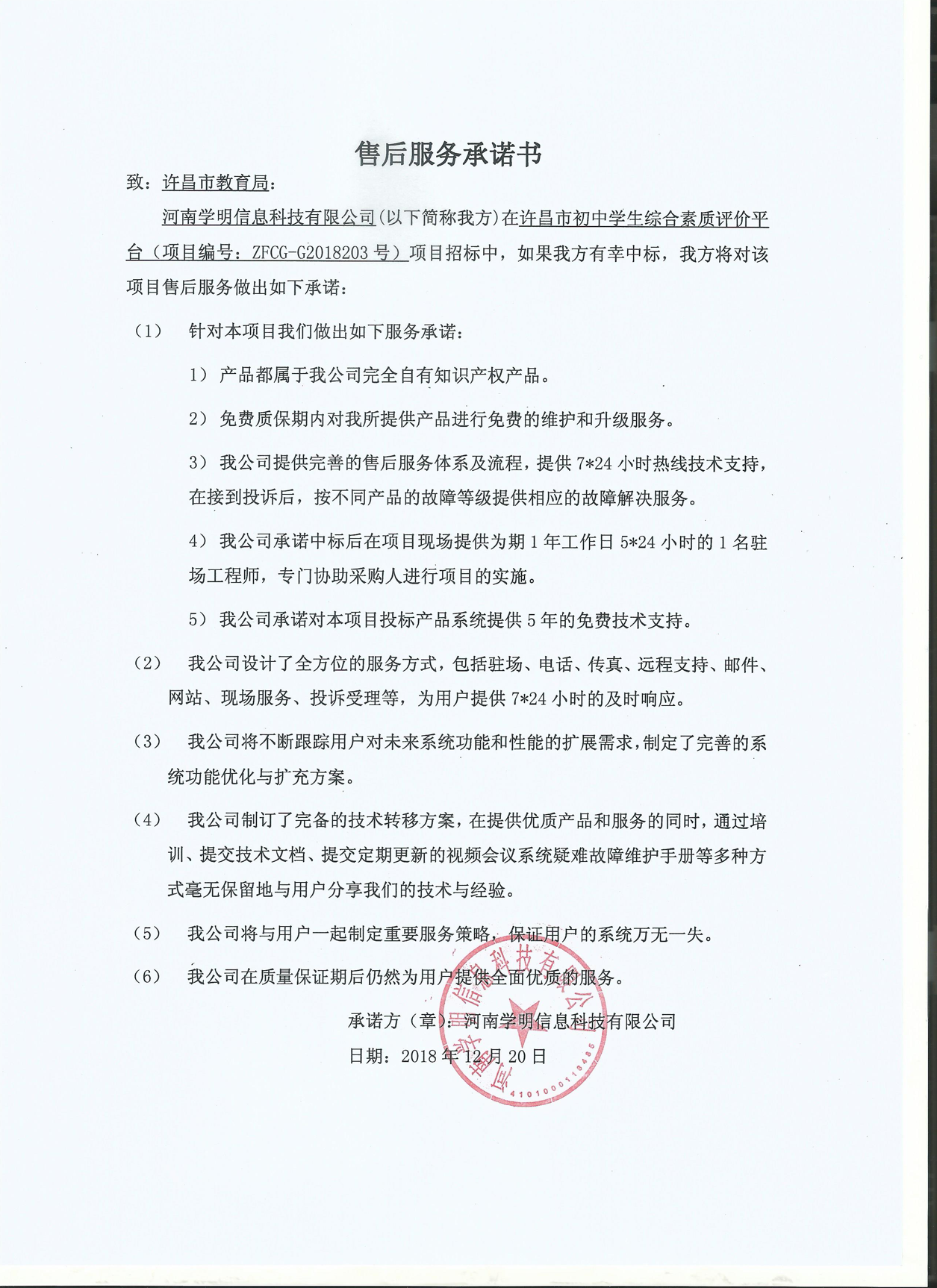
**4.4 售后服务方案**

**4.4.1售后服务承诺函**

**4.4.2售后服务承诺**

河南学明信息科技有限公司对本项目服务承诺：

1. 我公司为用户提供一级本地化服务，保证为用户提供快速响应的、高质量的服务。
2. 售后服务机构名称：河南学明信息科技有限公司技术支持中心

地点： 郑州高新技术产业开发区西三环路289号河南省国家大学科技园(东区)1号楼3单元4层

售后服务热线：0371-56087886

质量保证期：项目验收完成后5年免费售后服务；

响应时间：响应速度15分钟内，技术人员4小时内到达现场。

1. 针对本项目我们做出如下产品质量承诺：
2. 产品都属于我公司完全自有知识产权产品。
3. 质量问题的处理:免费质保期内对我所提供产品进行免费的维护和升级服务。
4. 质量投诉的处理：我方具有完善的售后服务机构，具备完善的售后服务体系及流程，提供7\*24小时热线技术支持，在接到投诉后，按不同产品的故障等级提供相应的故障解决服务。
5. 我方承诺中标后在项目现场提供为期1年工作日5\*24小时的1名驻场工程师，专门协助采购人进行项目的实施。
6. 有完善的质量保证措施。
7. 我方针对本项目在质保期内提供以下服务：
8. 电话技术支持服务
9. 现场技术服务
10. 定期巡查服务
11. 免费技术保障及升级服务
12. 跟踪服务
13. 我公司和设备厂商设计了全方位的服务方式，包括驻场、电话、传真、远程支持、邮件、网站、现场服务、投诉受理等，为用户提供7\*24小时的及时响应。
14. 我公司和设备厂商制定了完善的软件升级、技术故障排除、系统运行情况跟踪等方案和突发事件应急策略等，消除用户的后顾之忧。
15. 我公司将不断跟踪用户对未来系统功能和性能的扩展需求，制定了完善的系统功能优化与扩充方案。
16. 我公司制订了完备的技术转移方案，在提供优质产品和服务的同时，通过培训、提交技术文档、提交定期更新的视频会议系统疑难故障维护手册等多种方式毫无保留地与用户分享我们的技术与经验。
17. 我公司与设备厂商共同制定了重要服务策略，保证用户的系统万无一失。
18. 我公司在质量保证期后仍然为用户提供全面优质的服务。

**4.4.2.1质保期内的服务承诺**

我公司承诺对本项目整体系统提供5年的免费售后服务。

我们将确保在产品的质量保修期内，如果系统软件有改进、新增功能等，均将及时免费提供给业主使用，并免费提供相应的技术文件。

我们确保交付的产品能够按照业主的相关技术要求正常运行。

**4.4.2.2质保期外的服务承诺**

质保期满后，我公司将提供一套五年内的售后服务计划及费用清单。

在此次项目质保期满后，我公司将向用户提供一份维护系统正常运行的服务计划表。同时，我公司将以一个不高于本次合同价格的优惠价格向用户提供正常服务。

项目质保期满后，业主可以通过购买续保，获得更加优质的服务。

**4.4.3售后服务体系**

河南学明信息科技有限公司拥有专业的售后服务体系，技术人员由专业人员组成，服务过程严格遵照标准要求执行，确保能为客户提供高标准的技术服务。

为了保障本项目得以顺利地实施和系统稳定可靠地运行，我公司根据多年进行大型系统集成的经验并结合本项目的特点，制定了详细的售后服务方案。

本项目我公司为用户制定一套完整的、由我公司提供的技术支持与售后服务方案。

我公司和设备厂商承诺提供招标书要求的对本项目所提供产品的技术支持与售后服务，而且还将利用我们自身的优势一起为用户提供独具特色的优质服务：

我公司和监控设备厂商的客服中心将通力合作，通过多种方式，按照高质量高标准的服务体系竭诚为用户服务。

**4.4.4售后服务保障措施**

本着“用户至上，真诚服务”的宗旨，我们将为本项目提供完整的产品维护计划，包括服务的次数、时间、服务内容及紧急维修服务。主要包括如下内容：

* 为用户提供产品运行状况书面报告与改进性技术建议书等。
* 升级服务
* 资料提供服务
* 保修期内服务
* 保修期外服务
* 电话热线服务等

在维护期内，我公司对本次所采购产品每年至少提供两次免费预防性现场维护检查，维护招标人系统运作状况，确保系统在符合技术和环境的要求下运行，具体包括：

检测相关设备硬件，为客户提供配套硬件环境方案建议；

对系统产品进行维护、升级、优化配置等，提高系统安全性、稳定性；

咨询操作员，排除可能引起故障的隐患；

为用户提供产品状况书面报告与改进性技术建议书等。

**4.4.4.1现场服务**

针对本次采购项目，我公司提供的售后服务具体内容如下：

我公司为用户提供7\*24\*365的电话技术支持服务，从而充分体现专业化和本地化服务的优势，免费技术支持电话如下；

技术支持部：0371-56087886

我公司为用户提供电子邮件技术支持服务，技术支持电子邮箱为zb@51xueming.com

现场技术服务：我公司承诺在本项目中，如果通过电话支持和电子邮件支持仍旧不能解决问题，我公司将提供现场技术服务。

**4.4.4.2升级服务**

提供硬件升级的服务工作，免收人工费。

由低档机升至高档机，或增加系统上的主机构成各个子系统，或增加新的功能插件模块，我公司将以最优惠的价格提供升级服务。

**4.4.4.3资料提供服务**

定期将最新产品资料或技术资料通过信函或电子邮件的方式提供给用户。

如需其它最新资料，可通过服务热线，由我公司派专人送至用户。

**4.4.5故障响应及处理措施**

针对业主的逐项要求，我们特此一一承诺如下：

1. 帮助热线时间：

服务时间：7\*24小时

响应时间：15分钟相应，给出应急解决方案

服务电话：0371-56087886

1. 紧急支持服务：

服务时间：7\*24小时

响应时间：15分钟给予相应并提供应急解决方案，4小时内到达现场解决问题；

服务电话：0371-56087886

1. 定期巡查服务：

我们承诺在质保期内必须提供每年不少于4次的巡检和免费维护服务。

**4.4.6售后响应机制及应急事件处理计划书**

**4.4.6.1预防与预警机制**

1. 应急小组针对各种可能发生的信息系统突发事件，建立和完善预测预警机制。
2. 预警信息分为外部预警信息和内部预警信息两类。外部预警信息指信息系统外，突发的可能需要通信保障、安全防范，或可能对信息系统产生重大影响的事件警报。内部预警信息指信息系统网内的事故征兆或局部信息系统突发事故，可能对其他或整个网络造成重大影响的事件警报。
3. 应急小组要加强对信息系统的日常监测工作。监测的内容主要包括：
4. 局域网通讯性能与流量监控；
5. 网络设备和安全设备的操作记录、网络访问记录；
6. 服务器性能、数据库性能、应用系统性能等运行状态，以及备份存贮系统状态等；
7. 服务器操作系统、数据库安全审计记录、业务系统安全审计记录；
8. 计算机漏洞公告、网络漏洞扫描报告；
9. 病毒公告、防病毒系统报告；
10. 其他可能影响信息系统的预警内容。
11. 应急小组获得外部重大预警信息或通过监测获得内部预警信息后，应对预警信息加以分析，按照早发现、早报告、早处理的原则，对可能演变为严重事件的情况，部署相应的应对措施，通知相关部门做好预防和保障应急工作的各项准备工作，并及时报告首席信息官。

**4.4.6.2预应急响应程序**

1. 信息系统使用单位或人员发现信息系统突发事件后，应及时报告应急小组。应急小组及时组织相关人员查找故障原因，在短时间内（一般要在半小时以内）依据故障情形和修复时间进行初步判别，确定故障分类级别，较大（三级）及其以上的突发事件应报告副组长及组长。
2. 信息系统突发事件发生后，根据突发事件严重程度，由组长及时向公司高层汇报，公司根据需要指定特定小组或人员对新闻媒体发布相关信息，所指定的小组或人员应严格按照组长规定及要求对外发布信息，其他部门或个人不得擅自接受新闻媒体采访或对外发布自己的看法和意见。
3. 发生较大（三级）及其以上信息系统突发事件时，应急小组除向副组长、组长报告外，应立即通知相关业务部门。各业务部门应做好服务对象的解释和疏导工作。
4. 根据不同的事件以及事件的级别，采取相应措施进行应急处理。突发事件处理过程中，可以根据需要调整故障级别。
5. 网络攻击事件应急预案：
6. 当发现网络被非法入侵、网页内容被篡改，应用服务器的数据被非法拷贝、修改、删除，或有黑客正在进行攻击等现象时，使用者或管理者应断开网络，并立即报告应急小组。
7. 应急小组立即关闭相关服务器，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道，并及时清理系统、恢复数据和程序，尽快将系统和网络恢复正常。
8. 信息破坏事件应急预案：
9. 当发现信息被篡改、假冒、泄漏等事件时，信息系统使用单位或个人应立即通知应急小组。
10. 如被篡改或被假冒的数据正在使用过程，应急小组应立即通知相关影响的业务部门停止使用此组数据。
11. 应急小组通过跟踪应用程序、查看数据库安全审计记录和业务系统安全审计记录查找信息被破坏的原因和相关责任人。
12. 应急小组提出修正错误方案和措施，并将结果及时通知各相关业务部门。
13. 信息内容安全事件应急预案：
14. 当发现不良信息或网络病毒时，系统使用人员立即断开网线，终止不良信息或网络病毒传播，并报告应急小组。
15. 应急小组根据情况通告局域网内所有计算机用户，隔离网络，指导各计算机操作人员进行杀毒处理、清除不良信息，直至网络处于安全状态。
16. 网络故障事件应急预案：
17. 发生网络故障事件后，系统使用人员应及时报告应急小组。
18. 应急小组及时查清网络故障位置和原因，并予以解决。
19. 不能确定故障的解决时间或解决故障的期限并属较大（三级）及其以上的，应急小组应报告副组长、组长。
20. 服务器故障应急预案：
21. 自动应急切换：

为保障系统的稳定运行，各系统必须针对应用进行主备服务器配置，服务器故障后，可以自动切换到备用服务器运行，完成快速自动切换。应急小组确定故障设备及故障原因，并通知相关厂商处理硬件故障问题。

1. 手动应急切换：

部分无法使用、不适合或不适用自动切换的应急处理：

各系统必须进行主、备配置，故障出现后，值班人员确定故障，立即启动故障转移并向运维经理汇报，涉及数据库的必须先向运维经理汇报，由运维经理确认是否切换备机，不得擅自处理。

1. 不能确定故障的解决时间或解决故障的期限并属较大（三级）及其以上的，应急小组应报告副组长、组长。
2. 软件故障事件应急预案：
3. 发生计算机软件系统故障后，系统使用人员应立即保存数据，停止该计算机的业务操作，并将情况报告应急小组，不得擅自进行处理。
4. 应急小组应立刻派出技术人员进行处理，必要情况下，通知各业务部门停止业务操作和对系统数据进行备份。
5. 应急小组组织有关人员在保持原始数据安全的情况下，对计算机系统进行修复；修复系统成功后，利用备份数据恢复丢失的数据。
6. 灾害性事件应急预案：
7. 一旦发生灾害性事件，应急小组每一位成员都应有责任在第一时间进入机房抢救服务器及存储设备。
8. 应急小组对服务器及存储设备的损坏程序进行评估。如服务器损坏或存储设备损坏无法使用，立即联系相关厂商，进入维保服务程序。
9. 根据服务器或存储设备修复和恢复系统所需时间，由首席信息官小组决定是否启用备份设备。
10. 其他突发事件应急预案：

应急小组立刻派出技术人员进入现场，制定相应措施，根据实际情况灵活处理，并按要求报告副组长、组长。

**4.4.6.3后期处置**

1. 故障排除后，应急小组向相关部门发出故障解除、系统恢复正常运行通知及事件报告。
2. 系统恢复运行后，相关操作人员尽快通知业务部门对故障发生前所进行过的业务操作进行检查，核对业务数据是否正确或有无丢失，不正确或有丢失的应马上更正或补录，确保数据的正确和完整。对在故障期间采用手工受理的事项，应及时在系统中补充完善。
3. 副组长、组长组织有关人员及有关技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处理能力、恢复重建等问题进行全面调查评估，总结经验教训，完善信息系统应急处理预案，整改信息系统存在的隐患。
4. 副组长、组长对在信息系统应急事件处理中做出突出贡献的集体和个人，提出表彰奖励；对玩忽职守，造成不良影响或严重后果的，按有关规定提出处理意见，并依法依规提出处理意见建议，并追究其责任。对于二级及以上事件处理完毕后需形成书面报告，向信息化管理委员会进行专题汇报，并由信息化管理委员会进行责任判定并追责。
5. 事件报告需包含以下内容：事件原因、处理过程、结果、影响范围、事件持续时间（持续时间由受影响业务部门提供）、造成的财务损失（由财务系统评估）、事件报告编号等；由酒店事业部、财务系统、风控系统以及受影响的业务部门会签后，主送董办备案。

**4.4.6.4应急保障**

1. 信息系统应做好系统数据的备份工作，保证重要数据在受到破坏后可紧急恢复。预留一定数量的网络硬件设备和服务器，用于预防或应对信息系统突发事件。
2. 选择熟悉信息系统软硬件的专业公司作为信息系统应急处理的社会应急支援单位，提供技术支持和服务。信息系统服务器以及存储设备要与专业厂商签定维保协议，确备用设备的供应时间。
3. 强化信息安全宣传教育，提高信息安全防御意识。每年至少组织开展一次全局范围内的信息网络安全教育，提高全局职工信息安全防范意识和能力。
4. 在出现不可控、极其严重的情况下，信息系统可以经财务及CEO同意后，引入第三方资源来解决问题。
5. 严格遵守信息系统现行值班制度，不断完善值班、监控、反馈、日志、汇报和汇总等工作。