信息化运维费政府采购合同

包号/分包名称：01/ 信息化基础运维

甲　　方：　北京市公园管理中心综合事务中心

乙　　方：　北京数字认证股份有限公司

签 订 地 点 ：北京市公园管理中心综合事务中心

合同基本信息

甲方：北京市公园管理中心综合事务中心

法定代表人：刘景起

项目负责人：庄磊

通讯地址：北京市西城区西直门外大街 143 号

联系电话：010-68390364　　传真：010-68390364

乙方：北京数字认证股份有限公司

法定代表人：詹榜华

项目负责人：肖瑾

通讯地址：北京市海淀区北四环西路 68 号 1501

联系电话：（010）58045600　　传真：（010）58045678

甲方(采购人)： 北京市公园管理中心综合事务中心

乙方(中标人)： 北京数字认证股份有限公司

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律法规以及信息化运维费采购项目(项目名称) XHTC-FW-2025-0950 号（采购编号）采购文件的规定，合同各方经平等协商达成合同如下：

第一条 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：

一、 本合同书及附件

二、 中标通知书

三、 响应文件 （含澄清文件、报价文件）

四、 公开招投标文件 （含招投标文件补充通知）

第二条 采购内容

一、服务内容：详见附件。

二、服务要求：详见附件。

第三条 双方的责任和义务

一、甲方责任和义务：

1.甲方有权对合同规定范围内乙方的运行维护服务行为和质量进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。

2.根据本合同规定，按时向乙方支付应付服务费用。

3.国家法律、法规所规定由甲方承担的其它责任。

二、乙方责任和义务：

1．按照合同约定收取服务费，根据与甲方的协商结果获取合同外服务的合理费用。

2．乙方应按期完成项目工作，如因乙方原因导致项目工作延迟或停顿的，由乙方承担责任。

3．乙方承诺具有履行本合同的条件和资质，并投入合格的、充足的项目实施人员提供项目实施和服务保障。

4．严格履行合同文本（含采购文件、投标/响应文件等）约定和承诺的服务内容、质量标准、工序工艺，保障正常运行使用。

5．制定并执行严格的安全生产管理措施，保证甲乙方工作人员人身安全和甲方的设备设施

的完好无损。

6. 严格遵守国家法律，制定突发事件预案，合理合法地处置，杜绝恶性治安事件的发生。

第四条 服务期间（项目完成期限）

委托服务期间自 2025 年 07 月 01 日至 2026 年 06 月 30 日止。

第五条 验收方式

甲方依据本合同，在服务期满后 15 个工作日内对乙方服务情况进行验收。乙方应当在验收前向甲方提交相关工作材料。验收不合格的，乙方应当在 5 个工作日内进行返工或调整，并重新提交甲方验收。

第六条 合同价格及结算方式

1. 合同总金额为人民币 1,861,200.00 元（大写:壹佰捌拾陆万壹仟贰佰元整）。

2. 自合同签订后 30 个自然日内，甲方向乙方支付第一笔服务费（合同金额的 50%），即人民币小写：93.06 万元（人民币大写：玖拾叁万零陆佰元整）；2026 年 4 月 30 日前，甲方向乙方支付第二笔费用（合同金额的 25%），即人民币小写：46.53 万元（人民币大写：肆拾陆万伍仟叁佰元整）；服务期满后 30 个自然日内，甲方向乙方支付第三笔费用（即合同金额的 25%），即人民币小写：46.53 万元（人民币大写：肆拾陆万伍仟叁佰元整）。（按照奖惩措施，罚款金额在第三笔运维费中进行扣减，据实结算。）

3. 乙方账户信息

乙方开户名称：北京数字认证股份有限公司

乙方开户银行：北京银行双清苑支行

乙方开户账号：01090327800120102315712

乙方必须于甲方每次付款前提供相应项目金额的合法正规发票。否则甲方有权拒绝付款且不承担逾期付款违约责任。

第七条 知识产权责任

1. 乙方应保证本项目的技术、服务或其任何一部分不会产生因第三方提出侵犯其专利权、商标权或其他知识产权而引起的法律和经济纠纷；如因第三方提出其专利权、商标权或其他知识产权的侵权之诉，则一切法律责任由乙方承担。

2. 其他：无

第八条 不可抗力

一、不可抗力指下列事件：战争、动乱、瘟疫、严重火灾、洪水、地震、风暴或其他自然灾害，以及本合同各方不可预见、不可防止并不能避免或克服的一切其他事件。

二、任何一方因不可抗力不能履行本合同规定的全部或部分义务，该方应尽快通知另外一方，并须在不可抗力发生后三日内以书面形式向另外一方提供详细情况报告及不可抗力对履行本合同的影响程度的说明。

三、发生不可抗力事件，任何一方均不对因不可抗力无法履行或迟延履行本合同义务而使另外两方蒙受的任何损失承担责任。但遭受不可抗力影响的一方有责任尽可能及时采取适当或必要措施减少或消除不可抗力的影响。遭受不可抗力影响的一方对因未尽本项责任而造成的相关损失承担责任。

四、合同各方应根据不可抗力对本合同履行的影响程度，协商确定是否终止本合同，或是继续履行本合同。

第九条　联系方式

一、合同各方发出与本合同有关的通知或回复，应以专人送递、传真或特快专递方式发出；如果以专人送递或特快专递发送，以送达至对方的住所地或通讯联络地为送达；如果以传真方式发送，发件人在收到传真报告后视为送达。

二、合同各方发出的与本合同有关的通知或回复均应发至以下通讯地址，一方变更通讯地址或帐号，应自变更之日起三个工作日内，将变更后的地址通知对方。变更方不履行通知义务的，应对此造成的一切后果承担法律责任。

甲方：北京市公园管理中心综合事务中心　　联系人：牛锐

地址：　　邮编：

电话：　　传真：

乙方：北京数字认证股份有限公司　　联系人：肖瑾

地址：北京市海淀区北四环西路 68 号 1501　　邮编：100080

电话：（010）58045600　　传真：（010）58045678

上述发出通知、回复的费用由发出一方承担。

第十条 保密条款

一、任何一方对其获知的本合同及附件中其他各方的商业秘密和国家秘密负有保密义务。

二、除非法律、法规另有规定或得到本合同另一方的书面许可，任何一方不得向第三人（但双方聘请的律师除外）泄露前款规定的商业秘密和国家秘密。保密期限自任何一方获知该商业秘密和国家秘密之日起至本条规定的秘密成为公众信息之日止。

第十一条 合同的解释和法律适用

1.任何一方对本合同及其附件的解释均应遵循诚实信用原则,依照本合同签订时有效的中国法律、法规以及通常的理解进行。

2.本合同标题仅供查阅方便，并非对本合同的诠释或解释；

3.本合同中以日表述的时间期限均指自然日。

4.对本合同的任何解释均应以书面作出。

5.本合同及附件的订立、效力、解释、履行、争议的解决等适用本合同签订时有效的中华人民共和国法律、法规的有关规定。

第十二条 合同的终止

一、本合同因下列原因而终止：

1.本合同正常履行完毕；

2. 对本合同终止有过错的一方应赔偿另外一方因合同终止而受到的损失；

3.不可抗力事件导致本合同无法履行或履行不必要；

4.任何一方行使解除权，解除本合同。

二、对本合同终止有过错的一方应赔偿另外一方因合同终止而受到的损失。对合同终止各方均无过错的，则各自承担所受到的损失。

第十三条 争议的解决

1.合同各方应通过友好协商解决因解释、执行本合同所发生的和本合同有关的一切争议。如果经协商不能达成协议，则各方同意在甲方住所地有管辖权的人民法院提起诉讼。

2.在诉讼期间,除了必须在诉讼过程中进行解决的那部分问题外,合同其余部分应继续履行。

第十四条 合同的补充、修改和变更

1.双方协商一致，可以对本合同进行补充、修改或变更。

2.对本合同的任何补充、修改或变更必须以书面形式进行。

3.各方签订的补充协议以及修改或变更的条款与本合同具有同等法律效力。

第十五条 合同的生效

本合同经双方法定代表人（负责人）或授权代表签字并加盖单位公章后生效。

第十六条 其它约定事项

1.本合同未尽事宜，按照本招标文件的有关规定、中标人的中标文件及其澄清、说明或者补正文件执行。

2.本合同中的附件均为本合同不可分割的部分，与本合同具有相同的法律效力。

3. 一方当事人未经另对方书面同意，不得将其在合同项下的权利和义务全部或部分转让给第三人。

4. 本合同一式四份，每份具有同等法律效力。甲方两份，乙方两份。

合同附件一：《服务内容》

合同附件二：《服务要求》

合同附加三：《保密协议》

合同附件四：《合同履约考核表》

合同附件五：《奖惩措施》

（以下无正文）

甲方（采购人）：北京市公园管理中心综合事务中心

（公章）

法定代表或授权代表：

签订时间：2025 年 6 月 25 日

乙方（成交供应商）：北京数字认证股份有限公司

（公章）

法定代表或授权代表：

签订时间：2025 年 6 月 24 日

合同附件一：《服务内容》

1. 信息安全运维服务

随着网络和信息技术的快速发展和信息化的深入应用，我国各行业也在大力推动信息化发展，网络与信息系统建设已经成为各行业信息化的重中之重，信息化已经成为提高业务能力不可或缺的重要手段。但是信息化在发展的同时，也存在一些风险，例如当前网络攻击日益猖獗、攻击技术日新月异的安全形势，木马和僵尸网络、移动互联网恶意程序、拒绝服务攻击、安全漏洞、网页仿冒、网页篡改等网络安全事件越来越多，各行业面临着日益增长的网络安全威胁和信息安全挑战，形势严峻。

为加强甲方的网络安全工作。通过开展信息化安全服务，进一步完善甲方的安全保障体系，维持信息安全防护水平，保障业务系统的安全性及稳定性，保证甲方相关信息系统满足《网络安全法》等相关要求。

■ **服务范围**

本项目涉及的信息系统包括 OA 系统、用友财务系统、干部人才信息资源库、科技课题、北京市公园管理中心-动植物系统、古树古建系统、中心官网（公开招聘）、京办系统、杀毒系统等 9 个业务信息系统，涉及安全设备 26 台，网络设备 17 台，主机服务器 15 台，具体情况如下：

网络设备清单

序号	设备名称	备注
1	核心交换机	H3C S7703
2	汇聚交换机	H3C S5500
3	内网交换机-1	HUAWEI S5720S
4	内网交换机-2	HUAWEI S3600
5	内网交换机-3	HUAWEI S3700
6	内网交换机-4	HUAWEI S3700
7	内网交换机-5	HUAWEI S5735S
8	竖井内网交换机-6	HUAWEI S5720S
9	外网交换机-1	HUAWEI S5720S
10	外网交换机-2	HUAWEI S5735S

11	外网交换机-3	HUAWEI S3700
12	竖井外网交换机-4	HUAWEI S5720S
13	竖井外网交换机-5	HUAWEI S5735S
14	互联网 AP 交换机（1F）	信锐 RS5300
15	互联网 AP 交换机（2F）	信锐 RS5300
16	互联网 AP 交换机（3F）	信锐 RS5300
17	互联网 AP 交换机（4F）	信锐 RS5300

服务器设备清单

序号	设备用途	系统类型
1	OA 系统主服务器	Windows 2012 R2
2	OA 系统备用服务器 1	Windows 2012 R2
3	OA 系统备用服务器 2	Windows 2012 R2
4	用友财务服务器 1	Windows 2012 R2
5	用友财务服务器 2	Windows 2012 R2
6	科技课题管理系统服务器	Windows 2008 R2
7	干部人才信息库服务器	Windows 2008 R2
8	北京市公园管理中心-动植物系统	CentOS Linux release 7.6
9	古树信息系统	CentOS Linux release 7.4.
10	古树古建信息系统-服务器 1	CentOS Linux release 7.4.
11	古树古建信息系统-服务器 2	CentOS Linux release 7.4.
12	中心官网服务器	Windows 2008 R2
13	京办客流统计系统	CentOS Linux release 7.6
14	京办公园今日信息系统	CentOS Linux release 7.6
15	360 服务器	CentOS Linux release 7.6

安全设备清单

序号	设备名称	备注
1	无线网络控制器	信锐 NAC-6100
2	安全运营平台	安信天行
3	日志分析服务器	安信天行 V1.0-B-BJ
4	攻击预警平台 APT	明御 DAS-APT-1000
5	数据库审计服务器	安信天行 DBA/V1.0-2000
6	WEB 应用防火墙（天融信）	TopWAF(TWF-62128)
7	虚拟专用网络（VPN）平台	深信服 SSL M7.6.3
8	防病毒防火墙（政务外网区）	ADBJ-111
9	上网行为管理（政务外网区）	AS-VPBJ-210
10	外网入侵检测 IDS	华为 NIP6610
11	内网入侵检测 IDS	华为 NIP6610
12	政务网防火墙	华为 USG6100
13	直属公园网防火墙	华为 USG6000
14	直属园区边界防火墙（北海）	华为 USG6525E
15	直属园区边界防火墙（动物园）	华为 USG6525E
16	直属园区边界防火墙（香山）	华为 USG6525E
17	直属园区边界防火墙（国家植物园）	华为 USG6525E
18	直属园区边界防火墙（景山）	华为 USG6525E
19	直属园区边界防火墙（中山）	华为 USG6525E
20	直属园区边界防火墙（天坛）	华为 USG6525E
21	直属园区边界防火墙（陶然亭）	华为 USG6525E

序号	设备名称	备注
22	直属园区边界防火墙（颐和园）	华为 USG6525E
23	直属园区边界防火墙（玉渊潭）	华为 USG6525E
24	直属园区边界防火墙（园林学校）	华为 USG6525E
25	直属园区边界防火墙（园博馆）	华为 USG6525E
26	直属园区边界防火墙（紫竹院）	华为 USG6525E

1.1. 日常巡检服务

服务内容

乙方将利用检测工具和人工检测等多种方式定期对甲方信息系统的服务器、网络及安全设备的健康状态进行检测，包括设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作，做好巡检记录，维护记录单，提交巡检报告。

1.2. 应急响应服务

服务内容

乙方将针对病毒类安全事件、网络类安全事件和系统类安全事件开展应急响应工作。在信息安全事件发生时，能够保证网络与信息系统的正常运行。

1.3. 源代码审计服务

服务内容

源代码安全检测是通过对代码的检测，检查，识别发现代码中的安全漏洞，性能瓶颈，逻辑错误等问题，帮助开发人员在应用系统错误蔓延前发现问题。发现代码中有可能被恶意用户用来突破安全防护的缺陷。帮助开发人员建立起良好的编程规范，从底层解决了应用系统的安全问题。使用户更加真实的了解到信息系统的安全性状况。

1.4. 脆弱性检测服务

服务内容

乙方将派遣专业的服务人员对甲方信息系统的操作系统、数据库、中间件进行脆弱性检测，确保甲方可以定期掌握信息自身系统的脆弱性，初步定位信息系统弱点。

1.5. 漏洞扫描服务

服务内容

乙方将委派评估人员在获得甲方授权许可的前提下，将扫描工具接入网络内特定区域，设定合理检测策略，并选择非业务高峰时段对目标设备执行扫描。

1.6. 安全加固服务

服务内容

安全加固服务是为了消除信息系统自身的安全隐患，对目标系统实施全面而周到的安全配置，经过网络结构调整和设备配置优化，系统自身的抗攻击性也会有极大的增强。

根据本项目需求，安全加固服务内容包括：

安全加固服务包含网络结构优化调整、系统设备脆弱性加固、加固效果跟踪评价三部分工作。

1.7. 安全通告服务

1.7.1. 服务内容

信息安全通告服务，主要是依靠乙方的针对当前的信息安全态势、信息安全状况、技术发展趋势等信息进行收集，定期整理分析，并将信息安全分析结果以报告的形式发送客户方信息安全主管人员，以防范甲方内部信息安全事件的发生。

信息安全通告内容通常包括：本周信息安全疫情、专家预防建议、重点网站系统安全状况跟踪趋势、最新信息安全资讯、最新发布漏洞及解决建议、安全小常识等内容。

1.8. 安全驻场服务

服务内容

驻场工程师将承担应用系统运维商、基础环境运维商的信息安全监督角色，参与编制落实各种安全管理和安全技术规范，管理监督相关方落实，并对执行效果进行审核。乙方选派合格并符合甲方要求的安全服务人员（在工作量较大的情况下，将考虑增加人员配置）政治可靠、专业技术过硬、工作态度严谨踏实的专职人员全职参加用户的日常安全管理工作；驻场人员具备北京市委办局机关单位的安全运维服务经验；驻场人员将经过甲方的面试上岗，实行 5×8 小时工作制。

1.9. 设备维保服务

服务内容

乙方将对甲方指定的设备开展规则库升级以及维保工作，确保设备能够满足当前中心的网络安全需求，具体设备清单及需求如下：

序号	产品名称	产品型号	产品服务	单位	数量
1	VPN	VPN-1000-A400	软件升级	年	1
			维保服务	年	1
2	日志审计	AXTX-LM/V1.0-10000	分析规则库升级服务	年	1
			维保服务	年	1
3	明御 APT 攻击预警平台	DAS-APT-680	软件升级	年	1
			维保服务	年	1
4	华为防火墙 1	华为 USG6100	维保服务	年	1
5	华为防火墙 2	华为 USG6300	维保服务	年	1
6	华为入侵检测 1	华为 NIP6610	维保服务	年	1
7	华为入侵检测 2	华为 NIP6610	维保服务	年	1

8	内网流控	AS-VPBJ-210	网关杀毒升级许可	年	1
			深信服云智订阅软件（AF8.0.7及以上版本适用）	年	1
			软件升级	年	1
			维保服务	年	1
9	防毒墙	ADBJ-111	URL&应用识别规则库升级	年	1
			软件升级	年	1
			维保服务	年	1

1.10. 杀毒软件运维服务

服务内容

杀毒软件作为公园管理中心信息系统安全防线的关键一环，承担着保护整个单位计算机终端免受病毒侵害的重任。中心当前采用网络版杀毒软件，实现全面的病毒防护管理。乙方负责杀毒软件的安装部署、版本升级以及病毒库的及时更新，构建起坚实的防病毒屏障，确保信息系统免受病毒侵扰。此外，乙方提供定期的安全检测服务，对系统进行全面的病毒查杀，进一步保障系统的安全稳定运行。

2. 信息系统运维服务

2.1. OA 系统运维服务

服务内容

乙方将承担起 OA 系统的全面运维职责，包括日常的系统维护、故障快速排查与修复，以及系统的性能优化工作，同时紧跟技术发展步伐，密切关注系统升级和版本更新情况，及时引入最新的功能和服务。

详细服务内容如下：

总体运行维护服务

乙方负责对 OA 系统的全面运维服务，包括系统升级、操作系统安全维护、日常维护与安全加固、系统漏洞修复、数据库安全维护、客户端技术支持、服务器日志监控、数据库测试与分析、异构数据交换服务、数据库迁移服务。

1）系统升级：

乙方将依据办公 OA 系统的使用状况，优化系统性能，解决现存问题。在服务开展过程中，密切关注办公 OA 系统的实际使用情况，通过性能监控工具实时采集系统运行数据，全面梳理用户反馈的功能缺陷与操作卡顿等问题。基于数据诊断结果制定针对性优化方案，对系统代码进行重构、数据库索引优化及服务器资源调配，解决现有功能异常、响应迟缓等问题，同步提升系统稳定性与业务处理效率。

2）操作系统安全维护：

乙方将开展操作系统软件的安全检查、加固及维护工作。在服务开展过程中，定期开展操作系统软件的深度安全检查，通过漏洞扫描工具检测系统内核、服务组件等存在的安全隐患。针对检测结果实施安全加固，包括更新系统补丁修复已知漏洞、关闭非必要服务端口、优化安全策略配置，同时对系统关键文件进行加密保护，构建抵御恶意攻击的安全屏障，确保操作系统运行环境安全可控。

3）日常维护与安全加固：

乙方将强化 OA 系统的日常维护与安全加固工作。

一方面对现有系统进行日常维护，建立常态化维护机制，每日对现有系统进行巡检，及时处理登录异常、数据同步失败等日常故障，保障系统持续稳定运行。

另一方面对操作系统进行安全加固，具体措施包括：配置目录权限、组策略、本地安全策略；禁用未使用的服务；设置 IP 安全策略；对 IIS 进行加固。以上从多维度实施操作系统安全加固，严格配置目录权限防止数据非法访问，通过组策略与本地安全策略细化用户操作权限，禁用未使用的冗余服务减少攻击面，设置 IP 安全策略过滤非法访问请求，针对 IIS 服务进行专项加固，删除危险组件并优化访问规则。

4）系统漏洞修复：

乙方将定期针对操作系统自身存在的问题或技术缺陷，进行补丁更新。在服务开展过程中，构建定期漏洞管理机制，每月对操作系统进行全面漏洞扫描，结合 CVE 漏洞库评估漏洞风险等级。对高危及中危漏洞制定补丁更新计划，先在测试环境进行补丁兼容性测试，确认无异常后通过自动化部署工具实施批量更新，更新完成后再次扫描验证修复效果，形成漏洞发现-修复-验证的闭环管理流程。

5）数据库安全维护：

乙方将负责数据库的维护及安全性检查，涵盖：数据库日志记录、扩展存储过程管理、防范 TCP/IP 端口探测、限制网络连接 IP、数据库文件收缩、查询分析及性能分析，并提供索引建议。在服务开展过程中，全面负责数据库的日常维护与安全管控，实时监控数据库日志记录，及时发现并处理事务异常、权限违规等安全事件；严格管理扩展存储过程，禁用高危存储过程防止恶意代码执行；通过防火墙策略防范 TCP/IP 端口探测，设置白名单限制网络连接 IP 范围；定期进行数据库文件收缩释放存储空间，通过查询分析工具定位慢查询语句，开展性能分析并提供索引优化建议，保障数据库高效安全运行。

6）客户端技术支持：

乙方将为甲方的客户端提供现场及电话技术支持服务，解决客户端的软硬件问题。在服务开展工程中，当客户端出现软硬件问题时，可通过电话远程指导用户进行故障排查，如检查硬件连接、重启服务进程等。对于远程无法解决的问题，安排技术人员现场服务，快速诊断硬件故障并更换损坏部件，处理软件兼容性问题及系统崩溃修复，确保客户端设备正常使用。

7）服务器日志监控：

乙方将为 OA 系统服务器的监控日志进行分析，排查错误故障，处理警告级别日志，保存所有日志信息。同时，提供数据库的测试、转化服务。在服务开展过程中，建立服务器日志监控机制，实时分析系统日志、应用日志及安全日志，及时排查错误故障，对警告级别日志立即进行原因定位与处理，避免问题升级。采用日志管理系统集中保存所有日志信息，支持日志检索与审计，同时提供数据库的测试、转化服务，确保数据库在不同环境下的稳定性与兼容性。

8）数据库测试与分析：

乙方将提供数据库的测试、性能分析及报告服务。在服务开展过程中，运用专业测试工具对数据库进行全方位测试，包括压力测试、并发测试及备份恢复测试等，模拟高负载业务场景评估数据库性能表现。通过性能分析工具采集数据库运行指标，深入分析 CPU 占用、内存分配、磁盘 IO 等瓶颈问题，生成详细的性能分析报告，结合业务特点提供索引优化、查询语句调整等针对性建议，提升数据库整体性能。

9）异构数据交换服务：

乙方将提供异构数据的导入和导出服务。在服务开展过程中，提供高效的异构数据导入和导出服务，针对不同数据源设计数据转换规则，开发定制化接口实现数据格式标准化处理。在数据交换过程中严格把控数据完整性与一致性，支持批量数据处理与增量同步，解决不同系统间数据格式不兼容问题，实现数据的跨平台共享与交互。

10）数据库迁移服务：

乙方将提供数据库的迁移服务。在服务开展过程中，迁移前对源数据库进行全面评估，制定详细的迁移方案，包括迁移步骤、时间规划及风险预案。先对数据库进行完整备份，然后通过迁移工具将数据逐步迁移至目标环境，同步完成数据库对象的迁移与配置。迁移后进行全面测试，验证数据准确性与业务连续性，若出现异常可快速执行回滚方案，确保数据库迁移平稳完成。

定期巡检服务

乙方负责对 OA 系统开展定期应用巡检和检查，包括应用进程池、应用日志、应用进程、应用目录的完整性、系统用户状态及登录情况、系统的访问情况、应用缓冲池状态。

1）检查应用进程池：

通过监控工具查看进程池资源分配与运行状态，检测进程数量是否超出阈值、CPU 和内存占用是否异常，排查进程死锁、僵死或频繁重启等问题，确保进程池高效调度应用服务。

2）检查应用日志：

分析应用日志文件的完整性与连续性，检索错误/警告级别的日志记录，追踪异常操作时间戳与调用栈，核查日志滚动策略是否生效，避免因日志积压导致服务性能下降。

3）检查应用进程：

使用 ps 或 top 命令核查应用进程实例数，确认主进程与子进程状态，监控进程 CPU 使用率、内存驻留集大小，对比进程启动参数与配置文件的一致性。

4）检查应用目录的完整性：

校验应用安装目录下的二进制文件、配置文件及依赖库的 MD5/SHA256 哈希值，检查目录权限是否符合最小授权原则，扫描是否存在异常新增或缺失文件，防止文件篡改或损坏。

5）检查系统用户状态及登录情况：

查询系统用户列表的有效性，核实用户所属组与权限配置，分析 /var/log/secure 日志中的登录失败记录，追踪异常 IP 登录尝试，清理过期或未授权用户账号。

6）检查系统的访问情况：

通过 netstat 查看当前网络连接状态，分析 nginx/apache 等服务的访问日志，统计并发连接数与请求频率，核查防火墙规则是否拦截异常端口访问，检测 DDoS 攻击迹象。

7）检查应用缓冲池状态：

针对数据库或中间件缓冲池，监控缓存命中率、内存页交换频率及缓冲池等

待队列长度，检测是否存在缓冲池泄漏或配置参数不合理导致的性能瓶颈，优化缓冲池大小与淘汰策略。

操作系统定期巡检服务

乙方负责对 OA 系统操作系统开展定期巡检，包括 CPU 性能调控、内存使用状况管控、硬盘使用情况监控、系统进程调控、主机性能提升。

1） CPU 性能调控：

实时监测 CPU 使用率、负载峰值及核心温度，分析高频次运算场景下的调度瓶颈，通过调整进程优先级、优化内核调度策略，确保多任务并发时的资源均衡分配，同步生成 CPU 性能趋势报告以预判硬件升级需求。

2） 内存使用状况管控：

深度扫描内存占用分布，定位内存泄漏进程及碎片堆积模块，监控 swap 分区使用频率，通过调整内存回收参数、优化缓存策略释放冗余占用，对长期高负载进程进行内存映射分析并输出优化建议。

3） 硬盘使用情况监控：

巡检磁盘容量剩余空间、I/O 读写速率及响应延迟，读取 SMART 健康状态数据排查潜在坏道，清理系统日志及临时文件释放存储资源，对频繁读写的热数据路径进行磁盘碎片整理。

4） 系统进程调控：

遍历系统进程资源占用清单，识别 CPU/内存/磁盘异常占用进程，终止僵尸进程及恶意程序，优化开机启动项加载顺序，通过 cgroups 对关键进程进行资源限制，建立进程资源使用基线模型以快速定位突发异常。

5） 主机性能提升：

整合硬件监控数据与系统日志，从 CPU 频率动态调节、内存分页机制、磁盘缓存策略等维度生成性能优化方案，实施内核参数调优，通过压力测试验证优化效果并输出性能提升报告。

数据库定期巡检服务

乙方将每月对数据库执行一次全面备份，同时检查自动备份是否正常运行，并清理多余的备份记录，确保数据备份的可靠性。此外，定期巡检数据，包括优化性能、截断过大的数据库日志、清理过期日志等，具体内容如下：

1）检查文件系统、碎片、死锁以及占用 CPU 过高或执行时间过长的 SQL 语句。

2）监测表空间的使用情况。

3）检查数据库文件的 I/O 读写状况。

4）监控 Session 连接数量。

5）检测数据库监听的运行状态。

6）查看每日数据备份和数据同步是否正常。

7）监测报警日志。

8）对表和索引进行 Analyze，检查表空间碎片。

9）检测数据库后台进程。

10）监测数据库对象的空间扩展情况。

公文格式运维服务

乙方将根据甲方的要求，随时对以下公文格式进行更新和调整，具体范围包括但不限于：

■ **公文类型**

1）中心发文：涵盖中心党委文件、党政联合（党文）、中心发文、办公室文件、纪检委员会文件、机关总支部文件、党政联合文件、工会文件、机关委员会文件、纪律委员会文件、非紧急救助文件、精神文明建设领导小组文件、青年团文件，共计 13 种。

2）通知公告：包括中心通知、办公室通知、机关委员会通知、委员会通知、机关党委（党建工作处）通知，共计 5 种。

3）会议纪要：涉及主任会纪要、专项会纪要、行政会纪要、政工会纪要、机关总支部委员会纪要、常务专项会纪要、编委会会议纪要，共计 8 种。

4）下属单位上报中心的文件：每个单位的党委文件、行政文件、党政联合文件，共计 3 种。

✓ **调整内容**

1）对上述文件类型进行格式调整、打印格式更新。

针对格式调整与打印格式更新，将统一规范公文页面设置、字体字号及段落间距，细化版头、正文、附件等结构排版标准，同步更新页码、装订等打印参数要求，确保各类公文格式符合最新行业规范与中心内控标准。

2）新增公文模板、电子公章，调整字体等。

新增公文模板与电子公章时，按 13 类中心发文、5 类通知公告等类型定制标准化模板，嵌入经权威机构认证的电子公章系统，同步调整正文统一使用仿宋 GB2312 字体、标题加粗等格式，实现模板复用与电子签章的合规化管理。

3）包括其他业务功能模块的调整与完善。

业务功能模块调整完善工作中，将优化公文流转审批、自动归档、智能检索等模块功能，增加格式校验、密级标识自动生成等辅助功能，同步强化用户权限分级管理与操作日志追溯机制，提升公文处理系统的安全性与便捷性。

4）配合完成云上业务系统的部署、调试及技术支持等工作。

配合云上业务系统部署时，全程参与服务器环境搭建、系统对接调试及数据迁移工作，协助完成公文系统与云平台的兼容性测试，提供 7×24 小时技术支持解决部署中出现的接口异常、流程卡顿等问题，并对中心用户开展云系统操作培训。

其他维护服务

乙方在开展系统运维过程中，对甲方提出对 OA 系统的其他维护要求进行响应和解决，主要包括：

1）收集并采纳用户提出的改进建议，负责具体实施工作。

2）提供办公 OA 系统软件的新版本更新服务。

3）承担办公 OA 系统的技术支持职责。

4）负责办公 OA 系统栏目的调整与设置。

5）解决用户在使用过程中遇到的问题。

6）对办公 OA 系统内容的数据进行异地备份。

7）解答用户在使用过程中遇到的各种问题，并解决相关故障。

8）如甲方需要对接其他业务系统，配合完成技术对接工作，不限于接口开发、对接调试等技术支持等工作。其他经双方友好协商确定的事宜：除以上问题外，当使用者发现其他需要乙方帮助解决的问题时，乙方将及时响应，经双方协商后，制定方案，及时实施，解决问题。

2.2. 人事报表系统运维服务

服务内容

在日常维护工作中，乙方将提供日常 5×8 小时的技术支持服务，并在紧急情况下确保 7×24 小时的快速响应。在整个运维周期内，系统所处理的所有个人隐私及单位敏感信息均将受到严格保密措施的保护。乙方还将承担系统数据维护、报表自动生成及数据分析等关键服务，以确保人事数据的准确无误与完整性。此外，根据甲方的具体需求，乙方将定制开发符合其个性化要求的报表展示与数据分析功能。

详细服务内容如下：

日常维护服务

1)设立服务台：

乙方将通过多种渠道统一接收用户关于系统的各类服务请求。

2)功能讲解：

乙方将介绍模块功能，指导用户操作，但不代为完成具体业务操作。

3)业务解答：

乙方将在客户授权的前提下，解答初级业务问题并进行讲解。

4)系统漏洞处理：

乙方将处理因系统自身漏洞导致客户无法正常开展业务的问题。

5)系统故障处理：

乙方将应对因服务中断或无法正常运行而引发的投诉或警报。

6)权限/用户管理：

乙方将负责用户和权限的新增、变更等管理事务。

7)基础资料管理：

涉及单位、收支分类科目、非指标类科目、收费项目信息以及其他基础数据的新增或变更，仅限于前台可处理的问题。

8)系统数据服务：

乙方将定期进行数据备份，以及处理因系统问题或客户误操作导致的后台数据问题。

9)系统维护：

包括常用配置信息调整、系统参数优化、定期重启系统、清理缓存等。

10)后台支持：

乙方将协调总部或第三方供应商资源，协助解决相关问题。

巡检服务

1） 系统健康检查：

乙方将为客户的软件系统和数据库进行全面检查，提前发现潜在问题，提供运行状况诊断报告及优化建议。每月开展一次巡检服务。

2） 用户改进建议响应与实施：

当甲方对人事报表系统提出新的功能需求时，乙方将在 72 小时内做出响应并提出改进方案，之后双方协商一致后，根据实际工作量尽快推进改进措施的落实。

首先，乙方将与甲方进行详细沟通，深入理解需求背景、功能目标及预期效果，对需求的可行性、技术复杂度及对现有系统的影响进行全面评估，形成初步的需求分析文档。

双方协商一致后，乙方将制定出具体的改进方案。方案包含功能设计架构、开发计划、测试方案、风险预案等内容，明确各阶段的时间节点和责任人。经甲方确认后，立即组织人员按照方案推进改进措施的落实。

改进完成后，进行全流程测试，确保改进后的系统稳定运行。测试通过后，为相关操作人员提供操作培训和技术文档更新服务。持续跟踪系统运行情况，收集使用反馈，确保新功能完全满足甲方的业务需求。

技术支持服务

在人事报表系统的使用过程中，若出现流程、技术、结构、硬件等方面的问题，以及其他任何相关问题，或者发现软硬件故障，乙方将及时响应并提供相应的技术支持。

设计发布新报表服务

在使用该系统期间，若因政策调整或单位要求需要对报表格式或内容进行更新，乙方将在收到相关反馈后，在 72 小时内拟定更新方案，并与需求方进行沟通协商，完成报表更新设计。

其他服务

除了上述提到的问题，如果使用者在使用过程中发现其他需要乙方协助解决的问题，乙方将及时做出响应。在双方进行协商后，共同制定出相应的解决方案，并尽快付诸实施，以及时有效地解决问题。

2.3. 门户网站技术运维服务

服务内容

乙方将负责门户网站的内容更新、技术支持以及安全监测等工作，保障网站内容的时效性和准确性。此外，还将关注网站的访问量和用户体验，持续优化网站的性能与功能。

2.4. 网站编辑与页面设计服务

服务内容

北京市公园管理中心网站是展示形象、传递信息的重要平台。因此，乙方将关注网站内容的编辑及页面的设计工作。按照《北京市政府网站页面设计统一规范》、《北京市政府网站政府信息公开专栏管理规定》等市级要求，完成网站日常运行、页面管理等工作。

2.5. 干部人才信息资源库系统运维服务

服务内容

乙方针对甲方干部人才库所涉及的中间件、应用软件系统及云服务器关的服务器、操作系统、数据库等，承担定期巡检、基础维护、功能维护、技术支持、安全加固、应急处置等服务工作，包括每周开展运行状态巡检、可用性检查、数据检查等。

定期巡检

每周对以下内容进行检查，包括：运行状态巡检、可用性检查、数据检查等。

基础维护

工作内容包括：补丁安装、账户及权限管理、资源分析。

功能维护

工作内容包括：应用系统缺陷维护、功能完善、资源变更等。

技术支持

应用系统使用支持

为切实保障用户在使用我们系统过程中的顺畅体验，乙方构建了一套全方位、多渠道的支持服务体系，力求在第一时间响应并满足用户的各类咨询与需求。

故障排除

为保障用户在使用本系统过程中获得优质、高效的技术支持，提升用户体验，现就用户技术问题处理制定方案，回复及时率不低于 95%。

安全响应

漏洞整改

乙方配合进行安全检测、漏洞扫描等相关工作，对发现的系统漏洞及时进行整改。在安全检测及渗透测试等基础上，对系统进行安全策略增强，全面提升系

统的安全保障能力。

应急处置

应急预案的制定和修订

根据系统运维类别的特点，制定北京市公园管理中心干部人才库应急预案并做相关修订，配备相关应急资源，针对突发紧急情况，启动技术专家现场服务，必要时联合多方面专家进行联合分析诊断、事件定位与紧急处理，持续跟进直到问题完全解决。

制定标准化的应急响应服务流程，建立分级故障响应机制，明确组织结构及职责划分，按照应急预案开展应急演练。

应急演练

每年开展 2 次应急演练，演练内容包括：对北京市公园管理中心干部人才库的主要业务功能和业务数据备份与恢复。每次演练，制定详细的演练方案和演练计划，演练过程中记录具体演练流程，在演练结束后及时完成演练总结报告。

应急处置

当应用系统发生紧急事件后，安全运维服务团队根据事件现象进行分析和故障级别判断，按照相关应急预案响应并快速及时为甲方提供全方位的技术支持，帮助客户在最短时间内控制安全事件对系统造成的影响，确定安全事件的故障源及问题原因，并提供解决方案。

1. 一般性事件应急处置

一般性事件定义：现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响数据中心业务运作，持续小于 4 小时，造成一定范围的不良影响的事件。持续时间超过 4 小时则升级到重大事件。包括一般网站事件、严重网络事件、严重应用事件和基础设施故障等安全事件。

一般性事件服务响应：工作时间 1 小时之内启动应急响应，非工作时间 2 小时之内启动应急响应。

一般性事件处置：一般性事件在 4 小时之内完成业务恢复、备机启用。

2. 重大事件应急处置

重大事件定义：现有的系统宕机，或遭到严重攻击、入侵等行为，使业务系统无法正常提供服务、信息系统的正常业务运作产生重大影响，或严重影响到业务提供服务的服务质量的，造成大范围不良影响的重大事件。包括重大网络事件、网站事件、应用事件和严重的基础设施故障等安全事件。

重大事件服务响应：工作时间 10 分钟之内启动应急响应，非工作时间 20 分钟之内启动应急响应。

重大事件处置：重大事件在 30 分钟之内完成业务恢复、备机启用。

2.6. 科技课题管理系统运维服务

服务内容

定期巡检

每周对以下内容进行检查，包括：运行状态巡检、可用性检查、数据检查等。

基础维护

工作内容包括：补丁安装、账户及权限管理、资源分析。

功能维护

工作内容包括：应用系统缺陷维护、功能完善等。

技术支持

应用系统使用支持

乙方提供全方位、多渠道的支持，包括用户交流群、24 小时服务电话以及 QQ 在线即时通讯，确保随时响应并满足用户的咨询与需求。

故障排除

解决甲方在使用系统过程中遇到的技术问题，解决各公园在上报课题工作时，使用系统过程中遇到的技术问题。对于用户咨询和问题反馈，需在 24 小时内给予明确回复和解决方案，回复及时率不低于 95%。

安全响应

漏洞整改

配合进行安全检测、漏洞扫描等相关工作，对发现的系统漏洞及时进行整改。在安全检测及渗透测试等基础上，对系统进行安全策略增强，全面提升系统的安全保障能力。

应急处置

应急预案的制定和修订

根据系统运维类别的特点，制定北京市公园管理中心干部人才库应急预案并做相关修订，配备相关应急资源，针对突发紧急情况，启动技术专家现场服务，必要时联合多方面专家进行联合分析诊断、事件定位与紧急处理，持续跟进直到问题完全解决。

制定标准化的应急响应服务流程，建立分级故障响应机制，明确组织结构及职责划分，按照应急预案开展应急演练。

应急预案主要包括：

《干部人才库应急预案》

应急演练

每年开展 2 次应急演练，演练内容包括：对北京市公园管理中心干部人才库的主要业务功能和业务数据备份与恢复。每次演练，制定详细的演练方案和演练计划，演练过程中记录具体演练流程，在演练结束后及时完成演练总结报告。

应急处置

（1） 应急处置服务内容

当应用系统发生紧急事件后，安全运维服务团队根据事件现象进行分析和故障级别判断，按照相关应急预案响应并快速及时为甲方提供全方位的技术支持，帮助客户在最短时间内控制安全事件对系统造成的影响，确定安全事件的故障源及问题原因，并提供解决方案。

（2） 一般性事件应急处置

一般性事件定义：现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响数据中心业务运作，持续小于 4 小时，造成一定范围的不良影响的事件。持续时间超过 4 小时则升级到重大事件。包括一般网站事件、严重网络事件、严重应用事件和基础设施故障等安全事件。

一般性事件服务响应：工作时间 1 小时之内启动应急响应，非工作时间 2 小时之内启动应急响应。

一般性事件处置：一般性事件在 4 小时之内完成业务恢复、备机启用。

（3） 重大事件应急处置

重大事件定义：现有的系统宕机，或遭到严重攻击、入侵等行为，使业务系统无法正常提供服务、信息系统的正常业务运作产生重大影响，或严重影响到业务提供服务的服务质量的，造成大范围不良影响的重大事件。包括重大网络事件、网站事件、应用事件和严重的基础设施故障等安全事件。

重大事件服务响应：工作时间 10 分钟之内启动应急响应，非工作时间 20 分钟之内启动应急响应。

重大事件处置：重大事件在 30 分钟之内完成业务恢复、备机启用。

3. 机房设备维护方案

3.1. UPS 电源维护服务

服务内容

依据招标要求，乙方将针对 UPS 电源提供如下具体服务内容：

1. 7*24 小时技术支持；
2. UPS-每月度巡检一次（检查所有主控板电气连接是否安全可靠；检视输入/输出端子、螺栓、螺帽紧固性；检查 UPS 系统输入、输出空开容量是否符合规格；检查风扇运行状况，机内变压器、散热器等散热环境和通道情况；检查器件、电缆等是否有损坏、老化、过热情况；检查所有配件外观、紧固和泄漏情况；检查 UPS 运行环境(灰尘、温度、湿度等)是否符合要求；检查电池附近有无易燃、易爆、腐蚀性的物品或其它杂物；检查蓄电池连接是否紧固；检查蓄电池外壳是否变形；检查电池开关箱状态；）
3. 每年对 UPS 设备进行一次除尘清理；
4. 每月度检查电池组性能，每季度进行一次电池充放电实验并测试电池内阻；
5. 每年对 UPS 设备进行一次模拟电网故障测试；
6. 突发事件 4 小时到达现场并及时更换有问题的原厂新配件；
7. 每年年末对 UPS 整体性能进行检测，检测内容包括：

序号	名称	测试内容	具体数值	备注
1	控制系统			
2	整流器			
3	逆变器			
4	自动旁路			
5	电池			
6	电池开关			
7	充电部分			
8	结论			

3.2. 机房空调维护服务

服务内容

依据招标要求，乙方将针对 UPS 电源提供如下具体服务内容：

1. 7*24 小时技术支持服务；
2. 空调系统-设备档案及维保记录文档；
3. 空调系统每月度进行巡检（包含：市电电压、控制电压、高压运行压力、低压运行压力、压缩机电流、室内风机电流、加湿电流、冷凝风扇电流、冷凝风扇启动值、加湿排水、加湿上水、加热系统、冷凝器清洁状态、高压开关、低压开关、风量传感器、微电脑主控板、干燥过滤器、电磁阀状态、膨胀阀状态、显示屏、室内风机、室外风机、主电源开关、温湿度传感器、冷凝排水；风机相序、温度传感器、出风情况等）。负责对空调制冷剂的填充（如有泄露）；
4. 每月度清理空调加湿器系统，并更换加湿罐（加湿运行季节）；
5. 每月对空调室外机进行冲洗（4-9 月份）；
6. 突发事件 4 小时到达现场并及时更换有问题的原厂新配件；
7. 年度末对空调系统进行整体设备性能测试，性能测试的内容包括：

序号	名称	测试内容	具体数值	备注
1	控制系统			
2	压缩机			
3	室内风机			
4	加湿系统			
5	制冷循环系统			
6	室外风机			
7	加热系统			
8	结论			

3.3. 服务器运维服务

服务内容

服务器作为公园管理中心信息系统的基石，承载着关键的业务运行任务。目前，中心共有 13 台服务器，它们广泛支撑着办公系统、年票管理系统、报表生成系统、视频会议平台、财务办公平台以及古建信息系统的正常运行。

乙方将全面承担服务器的运维工作，包括日常维护、性能调优以及数据备份，以保障服务器的持续稳定运行和数据的安全无虞。此外，乙方还将密切关注服务器的硬件升级和扩容需求，为甲方提供灵活可扩展的硬件支持方案，确保信息系统能够随着业务需求的发展而不断升级和扩展。

3.4. 网络交换机、路由器、防火墙运维服务

服务内容

保障网络基础设施的稳定与安全运行，对交换机、路由器及防火墙的精心维护不可或缺。机房内配备了核心交换机两台、交换机共计 24 台、防火墙 6 台以及路由器 3 台，共同构建起坚实的网络架构。

乙方将构建一套全面而完善的网络设备维护体系，涵盖定期巡检、软硬件状态监控、预防性维护保养、安全策略更新与设备升级等多个维度。此外，乙方还将强化人员培训与技术支撑力度，确保网络设备能够持续安全、稳定地运行，为甲方的各项业务活动提供坚实可靠的网络保障。

4. 视频会议运维方案

4.1. 服务内容

（1）乙方保障公园管理中心和所属 15 家基层单位的视频会议系统正常会议召开。

（2）乙方保障公园管理中心与市委市政府之间电视电话会议召开。

（3）乙方保障公园管理中心与北京市应急管理局、北京园林绿化局之间电视电话会议召开。

合同附件二：《服务要求》

1. 项目背景

北京市公园管理中心（以下简称公园管理中心）为市政府直属正局级事业单位，负责市属公园及其他所属机构人、财、物管理。负责市属公园和其他所属机构的规划、建设、管理、保护、服务、科技工作，并实施监督，以及财务管理审计、劳动人事、安全保卫等工作。

为了确保系统及其他业务系统的平稳高效运行，保护项目已有投资，减少维护升级难度和降低维护成本，最大限度地降低系统风险。公园管理中心决定委托专业的公司提供信息安全运维服务、网站运维服务、机房设备维护、视频会议运维等服务，通过规范化的服务和技术支持，以保证系统正常运行和不断完善。

2. 服务地点及期限

服务地点：采购人指定地点。

服务期限：本项目服务期限为合同签订生效之日起 1 年。

3. 运维服务需求

3.1. 信息安全运维服务需求

随着网络和信息技术的快速发展和信息化的深入应用，我国各行业也在大力推动信息化发展，网络与信息系统建设已经成为各行业信息化的重中之重，信息化已经成为提高业务能力不可或缺的重要手段。但是信息化在发展的同时，也存在一些风险，例如当前网络攻击日益猖獗、攻击技术日新月异的安全形势，木马和僵尸网络、移动互联网恶意程序、拒绝服务攻击、安全漏洞、网页仿冒、网页篡改等网络安全事件越来越多，各行业面临着日益增长的网络安全威胁和信息安全挑战，形势严峻。为加强采购人的网络安全工作。通过开展信息化安全服务，进一步完善采购人的安全保障体系，维持信息安全防护水平，保障业务系统的安全性及稳定性，保证采购人相关信息系统满足《网络安全法》等相关要求。

3.1.1. 服务范围

本项目涉及的信息系统包括 OA 系统、用友财务系统、干部人才信息资源库、科技课题、北京市公园管理中心-动植物系统、古树古建系统、中心官网（公开招聘）、京办系统、杀毒系统等 9 个业务信息系统，涉及安全设备 26 台，网络设

备 17 台，主机服务器 15 台，具体情况如下：

网络设备清单

序号	设备名称	备注
1	核心交换机	H3C S7703
2	汇聚交换机	H3C S5500
3	内网交换机-1	HUAWEI S5720S
4	内网交换机-2	HUAWEI S3600
5	内网交换机-3	HUAWEI S3700
6	内网交换机-4	HUAWEI S3700
7	内网交换机-5	HUAWEI S5735S
8	竖井内网交换机-6	HUAWEI S5720S
9	外网交换机-1	HUAWEI S5720S
10	外网交换机-2	HUAWEI S5735S
11	外网交换机-3	HUAWEI S3700
12	竖井外网交换机-4	HUAWEI S5720S
13	竖井外网交换机-5	HUAWEI S5735S
14	互联网 AP 交换机（1F）	信锐 RS5300
15	互联网 AP 交换机（2F）	信锐 RS5300
16	互联网 AP 交换机（3F）	信锐 RS5300
17	互联网 AP 交换机（4F）	信锐 RS5300

服务器设备清单

序号	设备用途	系统类型
1	OA 系统主服务器	Windows 2012 R2
2	OA 系统备用服务器 1	Windows 2012 R2
3	OA 系统备用服务器 2	Windows 2012 R2
4	用友财务服务器 1	Windows 2012 R2
5	用友财务服务器 2	Windows 2012 R2

6	科技课题管理系统服务器	Windows 2008 R2
7	干部人才信息库服务器	Windows 2008 R2
8	北京市公园管理中心-动植物系统	CentOS Linux release 7.6
9	古树信息系统	CentOS Linux release 7.4.
10	古树古建信息系统-服务器 1	CentOS Linux release 7.4.
11	古树古建信息系统-服务器 2	CentOS Linux release 7.4.
12	中心官网服务器	Windows 2008 R2
13	京办客流统计系统	CentOS Linux release 7.6
14	京办公园今日信息系统	CentOS Linux release 7.6
15	360 服务器	CentOS Linux release 7.6

安全设备清单

序号	设备名称	备注
1	无线网络控制器	信锐 NAC-6100
2	安全运营平台	安信天行
3	日志分析服务器	安信天行 V1.0-B-BJ
4	攻击预警平台 APT	明御 DAS-APT-1000
5	数据库审计服务器	安信天行 DBA/V1.0-2000
6	WEB 应用防火墙（天融信）	TopWAF(TWF-62128)
7	虚拟专用网络（VPN）平台	深信服 SSL M7.6.3
8	防病毒防火墙（政务外网区）	ADBJ-111
9	上网行为管理（政务外网区）	AS-VPBJ-210
10	外网入侵检测 IDS	华为 NIP6610
11	内网入侵检测 IDS	华为 NIP6610
12	政务网防火墙	华为 USG6100
13	直属公园网防火墙	华为 USG6000

序号	设备名称	备注
14	直属园区边界防火墙（北海）	华为 USG6525E
15	直属园区边界防火墙（动物园）	华为 USG6525E
16	直属园区边界防火墙（香山）	华为 USG6525E
17	直属园区边界防火墙（国家植物园）	华为 USG6525E
18	直属园区边界防火墙（景山）	华为 USG6525E
19	直属园区边界防火墙（中山）	华为 USG6525E
20	直属园区边界防火墙（天坛）	华为 USG6525E
21	直属园区边界防火墙（陶然亭）	华为 USG6525E
22	直属园区边界防火墙（颐和园）	华为 USG6525E
23	直属园区边界防火墙（玉渊潭）	华为 USG6525E
24	直属园区边界防火墙（园林学校）	华为 USG6525E
25	直属园区边界防火墙（园博馆）	华为 USG6525E
26	直属园区边界防火墙（紫竹院）	华为 USG6525E

3.1.2. 服务需求

3.1.2.1. 日常巡检服务

服务需求：供应商需利用检测工具和人工检测等多种方式定期对采购人信息系统的服务器、网络及安全设备的健康状态进行检测，包括设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作，做好巡检记录，维护记录单，提交巡检报告。

服务范围：采购人的服务器、网络设备及安全设备，数量不少于 58 台。

服务频率：服务期内开展，1 次/月，共 12 次。

服务成果：《日常巡检报告》

3.1.2.2. 应急响应

服务需求：供应商需针对病毒类安全事件、网络类安全事件和系统类安全事件开展应急响应工作。在信息安全事件发生时，能够保证网络与信息系统的正常

运行。

服务范围：采购人 9 个业务信息系统。

服务频率：本项服务在服务期内，按需提供。

服务成果：《信息安全应急响应服务报告》。

3.1.2.3.源代码审计

服务需求：通过对源代码的检测、检查，识别并发现代码中存在的安全漏洞、性能瓶颈、逻辑错误等问题，帮助开发人员更好地了解信息系统的安全性状况，避免安全问题蔓延并指导应用系统开发商对系统进行改进。，并根据测试结果提供源代码审计报告。

服务范围：采购人指定的 1 个重要系统。

服务频率：服务期内开展，为采购人指定的 1 个重要系统开展 1 次源代码审计（含复测）服务。

服务成果：《源代码审计报告》。

3.1.2.4.脆弱性检测

服务需求：供应商需派遣专业的服务人员对采购人信息系统的操作系统、数据库、中间件进行脆弱性检测，确保采购人可以定期掌握信息自身系统的脆弱性，初步定位信息系统弱点。

服务范围：采购人的服务器，数量不少于 15 台。

服务频率：服务期内开展，1 次/年，共 1 次。

服务成果：《脆弱性检测报告》

3.1.2.5.漏洞扫描

服务需求：供应商需委派评估人员在获得采购人授权许可的前提下，将扫描工具接入网络内特定区域，设定合理检测策略，并选择非业务高峰时段对目标设备执行扫描。

服务范围：采购人的服务器、网络设备及安全设备，数量不少于 58 台。

服务频率：服务期内开展，1 次/年，共 1 次。

服务成果：《漏洞扫描报告》

3.1.2.6.安全加固

服务需求：供应商需根据前期脆弱性检查的结果，结合采购人的业务需求，

对采购人信息系统相关服务器的操作系统进行安全策略加强、调优等，提出合理加固方案并指导相应的实施，加强系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。

服务范围：采购人服务器的操作系统，数量不少于 15 台。

服务频率：服务期内开展，1 次/年，共 1 次。

服务成果：《信息系统安全加固报告》。

3.1.2.7. 安全通告

服务需求：供应商需跟踪最新的系统、网络和设备发现的安全问题，搜集整理的漏洞信息、系统补丁信息、病毒信息，及时有针对性地发布，确保采购人在第一时间内得到相关的网络安全信息，以此提高采购人的安全防范意识。

服务范围：采购人本级单位

服务频率：服务期内开展，2 次/月，共 24 次。

服务成果：《安全信息汇编》。

3.1.2.8. 安全驻场服务

服务需求：供应商需在服务期内指派安全工程师为采购人提供一周工作日 5*8 小时驻场服务，协助采购人进行网络和信息安全管理，负责网络与安全设备安全配置策略维护、病毒查杀、安全监测、设备运行状态检查、故障处置等事项，定期提供信息系统安全监测情况汇报，使各相关方能够实时掌握安全状况，随时应对和处理信息系统发生的各类安全事件，对设备进行有效的常规性安全维护，保障网络和系统处于“健康”、安全的状态。

服务范围：采购人本级单位

服务频率：服务期内派遣安全工程师提供 5*8 小时驻场服务。

服务成果：《信息安全现场保障工作报告》

3.1.2.9. 设备维保服务

服务需求：供应商需对以下设备开展规则库升级以及维保工作，确保设备能够满足当前中心的网络安全需求，具体设备清单及需求如下：

序号	产品名称	产品型号	产品服务	单位	数量
1	VPN	VPN-1000-A400	软件升级	年	1
			维保服务	年	1
2	日志审计	AXTX-LM/V1.0-10000	分析规则库升级服	年	1

			务		
			维保服务	年	1
3	明御 APT 攻击预警平台	DAS-APT-680	软件升级	年	1
			维保服务	年	1
4	华为防火墙 1	华为 USG6100	维保服务	年	1
5	华为防火墙 2	华为 USG6300	维保服务	年	1
6	华为入侵检测 1	华为 NIP6610	维保服务	年	1
7	华为入侵检测 2	华为 NIP6610	维保服务	年	1
8	内网流控	AS-VPBJ-210	网关杀毒升级许可	年	1
			深信服云智订阅软件（AF8.0.7 及以上版本适用）	年	1
			软件升级	年	1
			维保服务	年	1
9	防毒墙	ADBJ-111	URL&应用识别规则库升级	年	1
			软件升级	年	1
			维保服务	年	1

服务频率：服务期内按需提供。

服务成果：《安全设备维保记录》

3.1.2.10.杀毒软件运维需求

杀毒软件作为公园管理中心信息系统安全防线的关键一环，承担着保护整个单位计算机终端免受病毒侵害的重任。中心当前采用网络版杀毒软件，实现全面的病毒防护管理。供应商需负责杀毒软件的安装部署、版本升级以及病毒库的及时更新，构建起坚实的防病毒屏障，确保信息系统免受病毒侵扰。此外，供应商还应提供定期的安全检测服务，对系统进行全面的病毒查杀，进一步保障系统的安全稳定运行。

3.1.2.10.1.巡检服务

服务需求：供应商需每月开展一次远程巡检，内容涵盖：服务器和网络设备

的杀毒软件版本更新检查、日志审核、漏洞排查以及全面病毒扫描等。

服务频率：服务期内开展，1 次/月，共 12 次。

服务成果：《杀毒软件巡检服务报告》

3.1.2.10.2.升级服务

服务需求：由于采购人的特殊性质，所有网络系统必须具备高级别的安全防护。一旦恶意软件入侵，它可能会迅速在全网各个节点间传播，从而中断业务流程并破坏 IT 基础设施。服务器需要配备专门的安全解决方案，以保护关键数据免受恶意软件的威胁，确保在高负载条件下稳定运行，同时有效降低对系统资源的占用。此外，还需要及时更新和授权杀毒软件。供应商应定期进行病毒扫描检查，一旦发现杀毒软件有新版本发布或病毒库更新，应立即对全局病毒软件进行更新，并密切关注软件的使用期限，根据实际情况及时进行授权。

服务频率：服务期内按需开展。

服务成果：《杀毒软件升级服务记录》

3.1.2.10.3.客户端技术支持

服务需求：供应商需为采购人的所有客户端提供现场技术支持和电话技术支持，针对客户端出现的病毒问题提供相应的技术支持。

服务频率：服务期内按需开展。

服务成果：《杀毒软件客户端技术支持报告》

3.2.信息系统运维服务需求

3.2.1.OA 系统运维需求

技术指标要求：采购人的 OA 系统集成了通知公告、公文管理、会议纪要、收发文处理、局外来文管理以及电子邮件等多个核心模块，该系统已在中心及其下属单位广泛应用，成为日常办公不可或缺的平台。作为采购人内部办公的关键支撑，OA 系统的稳定运行是保障各项业务顺畅进行的基础。因此，供应商需承担起 OA 系统的全面运维职责，包括日常的系统维护、故障快速排查与修复，以及系统的性能优化工作，确保系统能够高效、稳定地运行。此外，供应商还需紧跟技术发展步伐，密切关注系统升级和版本更新情况，及时为采购人引入最新的功能和服务，以不断提升办公效率和体验。

运维服务需求：

序号	服务内容	具体描述	服务频率
1	总体运行维护要求	1）系统升级：依据办公 OA 系统的使用状况，优化系统性能，解决现存问题。 2）操作系统安全维护：开展操作系统软件的安全检查、加固及维护工作。 3）日常维护与安全加固：一方面对现有系统进行日常维护；另一方面对操作系统进行安全加固，具体措施包括：配置目录权限、组策略、本地安全策略；禁用未使用的服务；设置 IP 安全策略；对 IIS 进行加固。 4）系统漏洞修复：定期针对操作系统自身存在的问题或技术缺陷，进行补丁更新。 5）数据库安全维护：负责数据库的维护及安全性检查，涵盖：数据库日志记录、扩展存储过程管理、防范 TCP/IP 端口探测、限制网络连接 IP、数据库文件收缩、查询分析及性能分析，并提供索引建议。 6）客户端技术支持：为采购人的客户端提供现场及电话技术支持服务，解决客户端的软硬件问题。 7）服务器日志监控：监控服务器日志，排查错误故障，处理警告级别日志，保存所有日志信息。同时，提供数据库的测试、转化服务。 8）数据库测试与分析：提供数据库的测试、性能分析及报告服务。 9）异构数据交换服务：提供异构数据的导入和导出服务。 10） 数据库迁移服务：提供数据库的迁移服务。	服务期内按需开展。

2	定期巡检服务要求	1）检查应用进程池 2）检查应用日志 3）检查应用进程 4）检查应用目录的完整性 5）检查系统用户状态及登录情况 6）检查系统的访问情况 7）检查应用缓冲池状态	服务期内开展，1次/月，共12次。
3	操作系统定期巡检服务要求	1）CPU 性能调控 2）内存使用状况管控 3）硬盘使用情况监控 4）系统进程调控 5）主机性能提升	服务期内开展，1次/月，共12次。
4	数据库定期巡检服务要求	每月对数据库执行一次全面备份，同时检查自动备份是否正常运行，并清理多余的备份记录，确保数据备份的可靠性。此外，定期巡检数据，包括优化性能、截断过大的数据库日志、清理过期日志等，具体内容如下： 1）检查文件系统、碎片、死锁以及占用 CPU 过高或执行时间过长的 SQL 语句。 2）监测表空间的使用情况。 3）检查数据库文件的 I/O 读写状况。 4）监控 Session 连接数量。 5）检测数据库监听的运行状态。 6）查看每日数据备份和数据同步是否正常。 7）监测报警日志。 8）对表和索引进行 Analyze，检查表空间碎片。 9）检测数据库后台进程。 10）监测数据库对象的空间扩展情况。	服务期内开展，1次/月，共12次。
5	公文	根据采购人的要求，随时对以下公文格式进行更新和调	服务期

	格式运维要求	整，具体范围包括但不限于： **公文类型** 1）中心发文：涵盖中心党委文件、党政联合（党文）、中心发文、办公室文件、纪检委员会文件、机关总支部文件、党政联合文件、工会文件、机关委员会文件、纪律委员会文件、非紧急救助文件、精神文明建设领导小组文件、青年团文件，共计 13 种。 2）通知公告：包括中心通知、办公室通知、机关委员会通知、委员会通知、机关党委（党建工作处）通知，共计 5 种。 3）会议纪要：涉及主任会纪要、专项会纪要、行政会纪要、政工会纪要、机关总支部委员会纪要、常务专项会纪要、编委会会议纪要，共计 8 种。 4）下属单位上报中心的文件：每个单位的党委文件、行政文件、党政联合文件，共计 3 种。 **调整内容** 1）对上述文件类型进行格式调整、打印格式更新。 2）新增公文模板、电子公章，调整字体等。 3）包括其他业务功能模块的调整与完善。 4）配合完成云上业务系统的部署、调试及技术支持等工作。	内按需开展。
6	其他维护要求	1）收集并采纳用户提出的改进建议，负责具体实施工作。 2）提供办公 OA 系统软件的新版本更新服务。 3）承担办公 OA 系统的技术支持职责。 4）负责办公 OA 系统栏目的调整与设置。 5）解决用户在使用过程中遇到的问题。 6）采购人负责对办公 OA 系统内容的数据进行异地备份。	服务期内按需开展。

		7）解答用户在使用过程中遇到的各种问题，并解决相关故障。 8）如采购人需要对接其他业务系统，配合完成技术对接工作，不限于接口开发、对接调试等技术支持等工作。其他经双方友好协商确定的事宜：除以上问题外，当使用者发现其他需要供应商帮助解决的问题时，供应商应及时响应，经双方协商后，制定方案，及时实施，解决问题。	

服务成果：按照服务内容提供服务报告及相关记录表单。

3.2.2. 人事报表系统运维需求

技术指标要求：人事报表系统全面涵盖了采购人人力资源管理的各个层面。此系统旨在实现人事与薪酬的一体化集中管理，使财务人员能够便捷地添加、删除、修改及查询本单位人员信息及薪资数据，并对人事信息及薪资发放中的诸如应发工资总额等关键项目进行汇总与分类。同时，系统还具备强大的多维度查询功能，便于深入了解人事及薪酬管理状况。作为单位日常运作的核心系统之一，其重要性不言而喻。

因此，在日常维护工作中，供应商需承诺提供日常 5×8 小时的技术支持服务，并在紧急情况下确保 7×24 小时的快速响应。在整个运维周期内，系统所处理的所有个人隐私及单位敏感信息均将受到严格保密措施的保护。供应商还需承担系统数据维护、报表自动生成及数据分析等关键服务，以确保人事数据的准确无误与完整性。此外，根据采购人的具体需求，供应商还需定制开发符合其个性化要求的报表展示与数据分析功能。

运维服务需求：

序号	服务内容	具体描述	服务频率
1	日常维护需求	1）设立服务台：通过多种渠道统一接收用户关于系统的各类服务请求。 2）功能讲解：介绍模块功能，指导用户操作，但不代为完成具体业务操作。	服务期内按需开展

		3）业务解答：在客户授权的前提下，解答初级业务问题并进行讲解。 4）系统漏洞处理：处理因系统自身漏洞导致客户无法正常开展业务的问题。 5）系统故障处理：应对因服务中断或无法正常运行而引发的投诉或警报。 6）权限/用户管理：负责用户和权限的新增、变更等管理事务。 9）基础资料管理：涉及单位、收支分类科目、非指标类科目、收费项目信息以及其他基础数据的新增或变更，仅限于前台可处理的问题。 10）系统数据服务：定期进行数据备份，以及处理因系统问题或客户误操作导致的后台数据问题。 11）系统维护：包括常用配置信息调整、系统参数优化、定期重启系统、清理缓存等。 12）后台支持：协调总部或第三方供应商资源，协助解决相关问题。	
2	巡检服务需求	1）系统健康检查：为客户的软件系统和数据库进行全面检查，提前发现潜在问题，提供运行状况诊断报告及优化建议。每月开展一次巡检服务。 2）用户改进建议响应与实施：当采购人对人事报表系统提出新的功能需求时，供应商需在72小时内做出响应并提出改进方案，之后双方协商一致后，根据实际工作量尽快推进改进措施的落实。	服务期内开展，1次/月，共12次
3	技术支持工作需求	在人事报表系统的使用过程中，若出现流程、技术、结构、硬件等方面的问题，以及其他任何相关问题，或者发现软硬件故障，供应商需及时响应并提供相应的技术支持。	服务期内按需开展
4	设计	在使用该系统期间，若因政策调整或单位要求需要对报	服务期

	发布新的报表需求	表格式或内容进行更新，供应商在收到相关反馈后，需在 72 小时内拟定更新方案，并与需求方进行沟通协商，完成报表更新设计。	内按需开展
5	其他服务需求	除了上述提到的问题，如果使用者在使用过程中发现其他需要供应商协助解决的问题，供应商也应当及时做出响应。在双方进行协商后，共同制定出相应的解决方案，并尽快付诸实施，以及时有效地解决问题。	服务期内按需开展

服务成果：按照服务内容提供服务报告及相关记录表单

3.2.3. 门户网站技术运维需求

技术指标要求：采购人的门户网站是其对外宣传的关键平台。它主要负责发布市属公园及其他下属机构在规划、建设、管理、保护、服务和科技工作等方面的信息，为市民呈现北京的发展成果。该网站采用.NET 技术构建。供应商需负责门户网站的内容更新、技术支持以及安全监测等工作，保障网站内容的时效性和准确性。此外，还需关注网站的访问量和用户体验，持续优化网站的性能与功能。

运维服务需求：

序号	服务内容	具体描述	服务频率
1	巡检服务需求	系统性能的日常维护工作，每月一次的定期巡检。巡检的主要内容涵盖补丁的升级、日志的检查与分析，以及错误分析和统计。	服务期内开展，1 次/月，共 12 次
2	系统应急处理需求	系统故障检测与排除服务，承诺在 2 小时内对故障报警做出响应，并在 4 小时内完成故障的排查与修复工作，确保系统尽快恢复正常运行。	服务期内按需开展
3	二次	对于二次开发的相关需求，根据具体需求的复杂程度和	服务期

	开发相关需求	工作量进行评估。实施周期预计在5人天（即5个标准工作日）以内，可以直接进行开发和部署工作。这包括需求分析、设计、编码、测试以及最终的上线部署等环节，确保在规定的时间内高质量地完成开发任务，满足使用者的具体需求。	内按需开展
4	应用软件业务定制服务需求	在服务期间，针对采购人门户网站提供2个定制专题的制作服务	服务期内按需开展
5	系统备份服务需求	提供本机备份和异地备份两种方式，服务期内本机备份每天定时执行一次，异地备份每月人工备份一次	服务期内本机1次/天，共365次。异地备份1次/月，共12次

服务成果：按照服务内容提供服务报告及相关记录表单。

3.2.4. 网站编辑与页面设计服务需求

服务范围：采购人门户网站

服务需求：

北京市公园管理中心网站是展示形象、传递信息的重要平台。因此，本部分主要关注网站内容的编辑及页面的设计工作。需按照《北京市政府网站页面设计统一规范》、《北京市政府网站政府信息公开专栏管理规定》等市级要求，完成网站日常运行、页面管理等工作。服务需求包括但不限于：

（1）负责日常中心门户网站上信息公开内容的编辑、转发等服务性辅助工

作；

（服务频率：服务期内按需开展。）

（2）负责重点节假日及重点时期中心门户网站信息公开的编辑、转发等服务性辅助工作；

（服务频率：服务期内按需开展。）

（3）负责对中心门户网站上内容的调整与优化；

（服务频率：服务期内按需开展。）

（4）根据市级季度网站检查、安全检查等技术检查结果完成相关技术整改；

（服务频率：服务期内按需开展。）

（5）负责每月通过数据库、后台等方式，统计、汇总中心门户网站相关频道数据信息发布情况；

（服务频率：服务期内按需开展。）

（6）负责每季度完成市级政务公开网站自查辅助性技术工作，并对于重点问题提出合理性优化建议；

（服务频率：服务期内按需开展。）

（7）负责为中心门户网站按需制作专题、首页轮播图、活动页宣传图、网站首页设计等服务；

（服务频率：服务期内按需开展。）

（8）负责对中心门户网站首页、栏目、频道及广告头条等布局的调整与设计优化。

（服务频率：服务期内按需开展。）

（9）负责与首都之窗、政数局等市级部门业务对接人保持有效沟通，及时进行信息交互，确保整体工作开展顺利。

（服务频率：服务期内按需开展。）

服务成果：按照服务内容提供服务报告及相关记录表单。

3.2.5.干部人才信息资源库系统运维需求

服务范围：采购人的干部人才库部署在首信云，以租用云服务商服务方式解决网络基础设施、服务器计算和存储资源，以及网络安全防护、主机防病毒服务需求。本项目运维单位运维范围包括系统服务器、操作系统、数据库、中间件、应用系统，详细情况见下表。

序号	名称	数量	单位
一	服务器		
1	虚拟服务器	1	台
二	操作系统		
1	Windows Server 2008	1	套
三	数据库系统		
1	SQL Server 2014	1	套
四	中间件		
1	IIS	1	套
五	应用软件系统		
1	北京市公园管理中心干部人才库	1	套

服务需求：针对采购人干部人才库所涉及的中间件、应用软件系统及云服务器关的服务器、操作系统、数据库等，承担定期巡检、基础维护、功能维护、技术支持、安全加固、应急处置等服务工作，包括每周开展运行状态巡检、可用性检查、数据检查等，具体内容如下：

（一） 定期巡检

每周对以下内容进行检查，包括：运行状态巡检、可用性检查、数据检查等。

1. 运行状态巡检

对网络、主机、数据库、中间件、应用系统运行状态进行检查。

（1）网络监控

检查网络区域的网络策略是否正常，对外开放的网络服务是否正常，监控与对接的系统间的网络连通是否正常，检查网络流量、响应速度是否正常，记录监控日志，如发现异常及时上报处置。

（2）主机监控

检查服务器的运行状态，包括：系统日志、CPU 使用率、内存使用率、磁盘使用率，记录监控日志，如发现异常及时上报处置。

（3）数据库监控

检查数据库系统的运行状态，包括：数据库日志、连通状态、数据库连接数、查询效率、磁盘 I/O 读写速度，记录监控日志，如发现异常及时上报处置。

（4）中间件监控

检查 IIS 运行状态、应用池健康情况等，记录监控日志，如发现异常及时上报处置。

（5）应用系统巡检

检查重点功能运行状态，包括：北京市公园管理中心干部人才库及相关数据接口，记录运行日志，如发现异常及时上报处置。

2. 数据库巡检

包括数据库系统运行状态检查、数据库系统故障排除、数据库密码管理、数据库作业维护与管理等。

（1） 数据库系统运行状态检查

每周对数据库系统运行状态进行检查，通过数据库连接等方式，对数据库的连通性、数据库文件完整性、日志正常情况、数据库作业运行情况、数据库文件备份情况等进行检查。

（2） 数据库系统故障排除

对巡检发现的问题进行及时处理，并详细记录问题与处理过程，如遇重大故障，则按紧急预案流程进行处理。

（3） 数据库密码管理

对数据库的密码进行管理，每半年修改数据库的 SA 密码，确保数据库的安全性。

（4） 数据库作业维护与管理

制定数据库维护作业，备份配置文件、备份重要运行日志、清除过期日志、交易连接正常性测试。

3. 应用系统巡检

每周至少 2 次，安排专人人工检查应用系统交互功能，是否能够正常访问。

4. 月度巡检

每月至少进行 1 次全面检查，确保系统服务状态和健康指标达到既定标准，安全隐患发现率不低于 95%。

以上巡检内容需提交《巡检记录表》，巡检完成后，甲乙双方共同验收签字。

（二） 基础维护

工作内容包括：补丁安装、账户及权限管理、资源分析。

1. 补丁安装

每季度安装操作系统、数据库、中间件，并根据安全部门的警示通知及时安装相关补丁。

（1） 操作系统补丁安装

根据本项目运维范围内操作系统安全检查结果，制定详细的补丁加固计划与方案，对补丁进行兼容性测试，并对操作系统进行安全补丁加固，确保操作系统安全稳定运行。

（2） 数据库补丁安装

根据本项目运维范围内数据库安全检查结果，制定详细的补丁加固计划与方案，对补丁进行兼容性测试，并对数据库进行安全补丁加固，确保数据库安全稳定运行。

（3） 中间件补丁安装

根据中间件安全检查结果，制定详细的补丁加固计划与方案，对补丁进行兼容性测试，并对中间件进行安全补丁加固，确保中间件安全稳定运行。

2. 账户及权限管理

对本项目运维范围内包括机构管理、人员管理、权限管理功能应用支持。

（1） 人员管理

依据单位调整、单位用户增减变化情况，及时对系统用户进行新增、变更和删除，同时根据实际工作需要对用户账号、密码、所在单位、读写数据范围与权限以及功能角色进行授权与关联。由于人员变更及忘记密码的原因，支持用户找回或者重设密码。

（2） 权限管理

根据处室业务变化情况对系统角色进行增加、删除、合并、变更等调整，并

结合实际权限范围进行系统功能调整与配置。

3. 资源分析

每季度对网络、主机、数据库、中间件性能检查结果进行分析，对网络带宽、CPU、内存、磁盘空间进行合理化配置，制定《资源变更计划》和《实施方案》，提交资源变更申请，并跟踪资源变更情况。

（三） 功能维护

工作内容包括：应用系统缺陷维护、功能完善、资源变更等。

1. 应用系统缺陷维护

维护要求为：通过对应用系统的维护，分析用户提出的系统问题，分析应用系统对服务平台性能的要求，提出系统优化扩容解决方案，保障应用系统的处理服务性能。

问题的发现和确认：整理和确认使用中发现的问题和安全检查、系统安全等级保护测评中发现的应用系统不足。

原因分析和方案制定：分析确定原因，制定问题修复方案。

问题修复：及时安排有关的技术支持人员解决问题并进行与相关系统的功能联调。

结果验证：安排专人验证问题是否得到解决，由问题发现人员确认修复结果。

结果部署：按照流程将修复成果进行部署，与相关系统进行功能验证，进行回归测试并进行总结，跟踪运行情况，直至正常稳定运转。

2. 功能完善

整理和确认实际运转中各类用户提出的完善要求，分析需求。

制定完善方案，确定完善计划，及时安排技术支持人员进行功能完善并进行与相关系统的功能联调。

安排专人验证完善后的功能是否满足需求。

按照流程部署，与相关系统进行功能验证，进行回归测试并进行总结，跟踪功能运行情况，直至正常稳定运转。

（四） 技术支持

1. 应用系统使用支持

提供全方位、多渠道的支持，包括用户交流群、24 小时服务电话以及 QQ 在

线即时通讯，确保随时响应并满足用户的咨询与需求。

2. 故障排除

解决用户在使用系统过程中遇到的技术问题。对于用户咨询和问题反馈，需在 24 小时内给予明确回复和解决方案，回复及时率不低于 95%。

（五） 安全响应

1. 漏洞整改

配合进行安全检测、漏洞扫描等相关工作，对发现的系统漏洞及时进行整改。在安全检测及渗透测试等基础上，对系统进行安全策略增强，全面提升系统的安全保障能力。

（六） 应急处置

1. 应急预案的制定和修订

根据系统运维类别的特点，制定北京市公园管理中心干部人才库应急预案并做相关修订，配备相关应急资源，针对突发紧急情况，启动技术专家现场服务，必要时联合多方面专家进行联合分析诊断、事件定位与紧急处理，持续跟进直到问题完全解决。

制定标准化的应急响应服务流程，建立分级故障响应机制，明确组织结构及职责划分，按照应急预案开展应急演练。

应急预案主要包括：

《干部人才库应急预案》

2. 应急演练

每年开展 2 次应急演练，演练内容包括：对北京市公园管理中心干部人才库的主要业务功能和业务数据备份与恢复。每次演练，制定详细的演练方案和演练计划，演练过程中记录具体演练流程，在演练结束后及时完成演练总结报告。

3. 应急处置

（1） 应急处置服务内容

当应用系统发生紧急事件后，安全运维服务团队根据事件现象进行分析和故障级别判断，按照相关应急预案响应并快速及时为采购人提供全方位的技术支持，帮助客户在最短时间内控制安全事件对系统造成的影响，确定安全事件的故障源及问题原因，并提供解决方案。

（2） 一般性事件应急处置

一般性事件定义：现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响数据中心业务运作，持续小于 4 小时，造成一定范围的不良影响的事件。持续时间超过 4 小时则升级到重大事件。包括一般网站事件、严重网络事件、严重应用事件和基础设施故障等安全事件。

一般性事件服务响应：工作时间 1 小时之内启动应急响应，非工作时间 2 小时之内启动应急响应。

一般性事件处置：一般性事件需在 4 小时之内完成业务恢复、备机启用。

（3） 重大事件应急处置

重大事件定义：现有的系统宕机，或遭到严重攻击、入侵等行为，使业务系统无法正常提供服务、信息系统的正常业务运作产生重大影响，或严重影响到业务提供服务的服务质量的，造成大范围不良影响的重大事件。包括重大网络事件、网站事件、应用事件和严重的基础设施故障等安全事件。

重大事件服务响应：工作时间 10 分钟之内启动应急响应，非工作时间 20 分钟之内启动应急响应。

重大事件处置：重大事件需在 30 分钟之内完成业务恢复、备机启用。

服务指标要求：

编号	衡量项目	服务目标	计算方法
1	服务时间	远程运维 5×8 小时，应急响应 7×24 小时	日常运维服务时间为正常工作日周一到周五，不包括国家法定节假日，提供 7×24 小时应急响应服务。
2	客户投诉事件	≤2 次 每年	累计客户投诉事件次数
3	事故 4 小时内解决率	一级故障≥99%	一级故障≥99% 系统故障的个数/事件总个数×100% 注：事件处理记录
4	发生事故	一级事故≤1% 每年二级	出现故障个数/365 天

	率	事故≤2% 每年三级事故≤3% 每年	×100% 注：事件处理记录
5	重大故障次数	小于等于 2 次	全年重大故障即一级故障次数小于等于 2 次。
6	服务响应时间间	5×8 小时内，立即响应；5×8 小时外，10 分钟响应 30 分钟现场。	发现故障后立即进行响应；5×8 小时外，10 分钟响应，30 分钟现场
7	服务报告	每日巡检报告 每月服务月报	需要提交每日巡检数据的巡检报告；每月提交服务月报。
8	信息准确性	99%	所有系统软硬件信息资料库准确性 99%以上。

服务成果：

序号	工作内容	交付物名称
1	定期巡检	巡检记录表
2	基础维护	服务反馈单
3	功能维护	更新申请单
4	技术支持	运维工单
5	故障排除	
6	漏洞整改	漏洞整改报告
7	应急处置	应急响应总结报告
8	运维管理	月度工作总结
9		季度工作总结

3.2.6. 科技课题管理系统运维需求

服务范围：本项目部署在首信云，以租用云服务商服务方式解决网络基础设施、服务器计算和存储资源，以及网络安全防护、主机防病毒服务需求。本项目运维单位运维范围包括：系统服务器、操作系统、数据库、中间件、第三方组件、

应用系统，详细情况见下表。

服务需求：针对采购人科技课题系统所涉及的中间件、第三方组件、应用软件系统及云服务器关的服务器、操作系统、数据库等，承担定期巡检、基础维护、功能维护、技术支持、安全加固、应急处置等服务工作。

（一） 定期巡检

每周对以下内容进行检查，包括：运行状态巡检、可用性检查、数据检查等。

1. 运行状态巡检

对网络、主机、数据库、中间件、应用系统运行状态进行检查。

（1）网络监控

检查网络区域的网络策略是否正常，对外开放的网络服务是否正常，监控与对接的系统间的网络连通是否正常，检查网络流量、响应速度是否正常，记录监控日志，如发现异常及时上报处置。

（2）主机监控

检查服务器的运行状态，包括：系统日志、CPU 使用率、内存使用率、磁盘使用率，记录监控日志，如发现异常及时上报处置。

（3）数据库监控

检查数据库系统的运行状态，包括：数据库日志、连通状态、数据库连接数、查询效率、磁盘 I/O 读写速度，记录监控日志，如发现异常及时上报处置。

（4）中间件监控

检查 IIS 运行状态、应用池健康情况等，记录监控日志，如发现异常及时上报处置。

（5）应用系统巡检

检查重点功能运行状态，包括：北京市公园管理管理中心科技课题系统及相关数据接口，记录运行日志，如发现异常及时上报处置。

2. 数据库巡检

包括数据库系统运行状态检查、数据库系统故障排除、数据库密码管理、数据库作业维护与管理等。

（1） 数据库系统运行状态检查

每周对数据库系统运行状态进行检查，通过数据库连接等方式，对数据库的

连通性、数据库文件完整性、日志正常情况、数据库作业运行情况、数据库文件备份情况等进行检查。

（2） 数据库系统故障排除

对巡检发现的问题进行及时处理，并详细记录问题与处理过程，如遇重大故障，则按紧急预案流程进行处理。

（3） 数据库密码管理

对数据库的密码进行管理，每半年修改数据库的SA密码，确保数据库的安全性。

（4） 数据库作业维护与管理

制定数据库维护作业，备份配置文件、备份重要运行日志、清除过期日志、交易连接正常性测试。

3. 应用系统巡检

每周至少2次，安排专人人工检查应用系统交互功能，是否能够正常访问。

4. 月度巡检

每月至少进行1次全面检查，确保系统服务状态和健康指标达到既定标准，安全隐患发现率不低于95%。

以上巡检内容需提交《巡检记录表》，巡检完成后，甲乙双方共同验收签字。

（二） 基础维护

工作内容包括：补丁安装、账户及权限管理、资源分析。

1. 补丁安装

每季度安装操作系统、数据库、中间件，并根据安全部门的警示通知及时安装相关补丁。

（1） 操作系统补丁安装

根据本项目运维范围内操作系统安全检查结果，制定详细的补丁加固计划与方案，对补丁进行兼容性测试，并对操作系统进行安全补丁加固，确保操作系统安全稳定运行。

（2） 数据库补丁安装

根据本项目运维范围内数据库安全检查结果，制定详细的补丁加固计划与方案，对补丁进行兼容性测试，并对数据库进行安全补丁加固，确保数据库安全稳

定运行。

（3） 中间件补丁安装

根据中间件安全检查结果，制定详细的补丁加固计划与方案，对补丁进行兼容性测试，并对中间件进行安全补丁加固，确保中间件安全稳定运行。

2. 账户及权限管理

对本项目运维范围内包括机构管理、人员管理、权限管理功能应用支持。

（1） 人员管理

依据单位调整、单位用户增减变化情况，及时对系统用户进行新增、变更和删除，同时根据实际工作需要对用户账号、密码、所在单位、读写数据范围与权限以及功能角色进行授权与关联。由于人员变更及忘记密码的原因，支持用户找回或者重设密码。

（2） 权限管理

根据处室及各公园业务变化情况对系统角色进行增加、删除、合并、变更等调整，并结合实际权限范围进行系统功能调整与配置。

3. 资源分析

每季度对网络、主机、数据库、中间件性能检查结果进行分析，对网络带宽、CPU、内存、磁盘空间进行合理化配置，制定《资源变更计划》和《实施方案》，提交资源变更申请，并跟踪资源变更情况。

（三） 功能维护

工作内容包括：应用系统缺陷维护、功能完善、资源变更等。

1. 应用系统缺陷维护

维护要求为：通过对应用系统的维护，分析用户提出的系统问题，分析应用系统对服务平台性能的要求，提出系统优化扩容解决方案，保障应用系统的处理服务性能。

问题的发现和确认：整理和确认使用中发现的问题和安全检查、系统安全等级保护测评中发现的应用系统不足。

原因分析和方案制定：分析确定原因，制定问题修复方案。

问题修复：及时安排有关的技术支持人员解决问题并进行与相关系统的功能联调。

结果验证：安排专人验证问题是否得到解决，由问题发现人员确认修复结果。

结果部署：按照流程将修复成果进行部署，与相关系统进行功能验证，进行回归测试并进行总结，跟踪运行情况，直至正常稳定运转。

2. 功能完善

整理和确认实际运转中各类用户提出的完善要求，分析需求。

制定完善方案，确定完善计划，及时安排技术支持人员进行功能完善并进行与相关系统的功能联调。

安排专人验证完善后的功能是否满足需求。

按照流程部署，与相关系统进行功能验证，进行回归测试并进行总结，跟踪功能运行情况，直至正常稳定运转。

（四） 技术支持

1. 应用系统使用支持

提供全方位、多渠道的支持，包括用户交流群、24 小时服务电话以及 QQ 在线即时通讯，确保随时响应并满足用户的咨询与需求。

2. 故障排除

解决采购人在使用系统过程中遇到的技术问题，解决各公园在上报课题工作时，使用系统过程中遇到的技术问题。对于用户咨询和问题反馈，需在 24 小时内给予明确回复和解决方案，回复及时率不低于 95%。

（五） 安全响应

1. 漏洞整改

配合进行安全检测、漏洞扫描等相关工作，对发现的系统漏洞及时进行整改。在安全检测及渗透测试等基础上，对系统进行安全策略增强，全面提升系统的安全保障能力。

（六） 应急处置

1. 应急预案的制定和修订

根据系统运维类别的特点，制定北京市公园管理中心科技课题系统应急预案并做相关修订，配备相关应急资源，针对突发紧急情况，启动技术专家现场服务，必要时联合多方面专家进行联合分析诊断、事件定位与紧急处理，持续跟进直到问题完全解决。

制定标准化的应急响应服务流程，建立分级故障响应机制，明确组织结构及职责划分，按照应急预案开展应急演练。

应急预案主要包括：

《科技课题系统应急预案》

《系统数据接口应急预案》

2. 应急演练

每年开展 2 次应急演练，演练内容包括：对北京市公园管理中心科技课题系统的主要业务功能和业务数据备份与恢复。每次演练，制定详细的演练方案和演练计划，演练过程中记录具体演练流程，在演练结束后及时完成演练总结报告。

3. 应急处置

（1） 应急处置服务内容

当应用系统发生紧急事件后，安全运维服务团队根据事件现象进行分析和故障级别判断，按照相关应急预案响应并快速及时为采购人提供全方位的技术支持，帮助采购人在最短时间内控制安全事件对系统造成的影响，确定安全事件的故障源及问题原因，并提供解决方案。

（2） 一般性事件应急处置

一般性事件定义：现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响数据中心业务运作，持续小于 4 小时，造成一定范围的不良影响的事件。持续时间超过 4 小时则升级到重大事件。包括一般网站事件、严重网络事件、严重应用事件和基础设施故障等安全事件。

一般性事件服务响应：工作时间 1 小时之内启动应急响应，非工作时间 2 小时之内启动应急响应。

一般性事件处置：一般性事件需在 4 小时之内完成业务恢复、备机启用。

（3） 重大事件应急处置

重大事件定义：现有的系统宕机，或遭到严重攻击、入侵等行为，使业务系统无法正常提供服务、信息系统的正常业务运作产生重大影响，或严重影响到业务提供服务的服务质量的，造成大范围不良影响的重大事件。包括重大网络事件、网站事件、应用事件和严重的基础设施故障等安全事件。

重大事件服务响应：工作时间 10 分钟之内启动应急响应，非工作时间 20

分钟之内启动应急响应。

重大事件处置：重大事件需在 30 分钟之内完成业务恢复、备机启用。

服务指标要求：

编号	衡量项目	服务目标	计算方法
1	服务时间	远程运维 5×8 小时，应急响应 7×24 小时	日常运维服务时间为正常工作日周一到周五，不包括国家法定节假日，提供 7×24 小时应急响应服务。
2	客户投诉事件	≤2 次 每年	累计客户投诉事件次数
3	事故 4 小时内解决率	一级故障≥99%	一级故障≥99% 系统故障的个数/事件总个数×100% 注：事件处理记录
4	发生事故率	一级事故≤1% 每年二级事故≤2% 每年三级事故≤3% 每年	出现故障个数/365 天×100% 注：事件处理记录
5	重大故障次数	小于等于 2 次	全年重大故障即一级故障次数 小于等于 2 次。
6	服务响应时间间	5×8 小时内，立即响应； 5×8 小时外，10 分钟响应 30 分钟现场。	发现故障后立即进行响应；5×8 小时外，10 分钟响应，30 分钟现场
7	服务报告	每日巡检报告 每月服务月报	需要提交每日巡检数据的巡检报告；每月提交服务月报。
8	信息准确性	99%	所有系统软硬件信息资料库准确性 99%以上。

服务成果：

序号	工作内容	交付物名称
1	定期巡检	巡检记录表
2	基础维护	服务反馈单
3	功能维护	更新申请单
4	技术支持	运维工单
5	故障排除	
6	漏洞整改	漏洞整改报告
7	应急处置	应急响应总结报告
8	运维管理	月度工作总结
9		季度工作总结

3.3.机房设备维护

3.3.1.UPS 电源维护需求

服务需求：供应商需提供 1、7*24 小时技术支持；2、UPS-每月度巡检一次（检查所有主控板电气连接是否安全可靠；检视输入/输出端子、螺栓、螺帽紧固性；检查 UPS 系统输入、输出空开容量是否符合规格；检查风扇运行状况，机内变压器、散热器等散热环境和通道情况；检查器件、电缆等是否有损坏、老化、过热情况；检查所有配件外观、紧固和泄漏情况；检查 UPS 运行环境(灰尘、温度、湿度等)是否符合要求；检查电池附近有无易燃、易爆、腐蚀性的物品或其它杂物；检查蓄电池连接是否紧固；检查蓄电池外壳是否变形；检查电池开关箱状态；）3、每年对 UPS 设备进行一次除尘清理；4、每月度检查电池组性能，每季度进行一次电池充放电实验并测试电池内阻；5、每年对 UPS 设备进行一次模拟电网故障测试；6、突发事件 4 小时到达现场并及时更换有问题的原厂新配件；7、每年年末对 UPS 整体性能进行检测，检测内容包括但不限于：

序号	名称	测试内容	具体数值	备注

1	控制系统			
2	整流器			
3	逆变器			
4	自动旁路			
5	电池			
6	电池开关			
7	充电部分			
8	结论			

服务范围：

序号	名称	型号	数量	使用年限
1	UPS 电源	索克曼 40KVA	1	约 8 年
2	电池	12V-100AH	40	5 年
3	电池开关	索克曼	1	约 8 年

服务频率：按需提供。

服务成果：《UPS 电源维护服务报告》

3.3.2. 机房空调维护需求

服务需求：供应商需提供的服务内容包括 1、7*24 小时技术支持服务；2、空调系统-设备档案及维保记录文档；3 空调系统每月度进行巡检（包含：市电电压、控制电压、高压运行压力、低压运行压力、压缩机电流、室内风机电流、加湿电流、冷凝风扇电流、冷凝风扇启动值、加湿排水、加湿上水、加热系统、冷凝器清洁状态、高压开关、低压开关、风量传感器、微电脑主控板、干燥过滤器、电磁阀状态、膨胀阀状态、显示屏、室内风机、室外风机、主电源开关、温湿度传感器、冷凝排水；风机相序、温度传感器、出风情况等）。负责对空调制冷剂的填充（如有泄露）；4、每月度清理空调加湿器系统，并更换加湿罐（加湿运行季节）；5、每月对空调室外机进行冲洗（4-9 月份）；6、突发事件 4 小时到

达现场并及时更换有问题的原厂新配件；7、年度末对空调系统进行整体设备性能测试，性能测试的内容包括：

序号	名称	测试内容	具体数值	备注
1	控制系统			
2	压缩机			
3	室内风机			
4	加湿系统			
5	制冷循环系统			
6	室外风机			
7	加热系统			
8	结论			

服务范围：

序号	名称	型号	数量	使用年限
1	机房空调	维谛 DM12	1	约 8 年
2	机房空调	维谛 DM12	1	约 6 年

服务频率：服务期内按需提供。

服务成果：《机房空调维护服务报告》

3.3.3. 服务器运维需求

服务器作为公园管理中心信息系统的基石，承载着关键的业务运行任务。目前，中心共有 13 台服务器，它们广泛支撑着办公系统、年票管理系统、报表生成系统、视频会议平台、财务办公平台以及古建信息系统的正常运行。

供应商需全面承担服务器的运维工作，包括日常维护、性能调优以及数据备份，以保障服务器的持续稳定运行和数据的安全无虞。此外，供应商还需密切关注服务器的硬件升级和扩容需求，为采购人提供灵活可扩展的硬件支持方案，确

保信息系统能够随着业务需求的发展而不断升级和扩展。

3.3.3.1.巡检服务

服务需求：

检查服务器运行状况：查看系统日志，分析并解决错误提示，检查系统磁盘空间及其变化，查看数据备份情况，监测 CPU 使用率和系统内存使用情况。

检查机房服务器及存储硬盘指示灯：若指示灯报红或报黄，排查原因。如硬盘损坏或即将损坏，及时更换相应硬盘。

检查系统补丁更新情况。

检查活动目录的复制状态。

审核管理组成员资格。

执行验证恢复操作，检测备份的可靠性。

检查活动目录数据库的大小和完整性。

检查 DHCP 服务范围，确保有足够可用的 IP 地址。

定期检查磁盘目录，并对系统进行碎片整理。

定期进行系统状态备份。

服务频率：服务期内开展，1 次/月，共 12 次。

服务成果：《服务器巡检服务报告》

3.3.3.2.故障排除与应急响应

服务需求：供应商需在服务器的维护工作中，负责故障排除和应急响应。对于巡检过程中发现的故障或采购人上报的故障，应迅速进行处理，以最大程度减少对服务器运行的影响。一旦发现问题，需立即着手解决，并及时上报相关情况。在处理过程中，必须确保不影响单位系统的正常运行。若需要对服务器进行更新部署操作，应严格遵循流程，完成上报审批手续。对于紧急故障，提供 8 小时内上门服务。

服务频率：服务期内按需开展。

服务成果：《服务器故障排除与应急响应报告》

3.3.3.3.备件服务

服务需求：提供易耗件及备件的更换服务，保障服务器的稳定运行。若发现配件老化或损坏，若有备件库存，将第一时间完成更换；若无备件可用，供应商

应负责修复后再进行更换。

服务频率：服务期内按需开展。

服务成果：《服务器备品备件清单》

3.3.3.4.扩容服务

服务需求：

系统扩容服务：当系统因数据量增加需要扩大服务器硬盘容量时，供应商需提供扩容方案，并依据双方协商结果执行扩容操作。

扩容实施时间：扩容操作应尽量安排在公休时间进行。

软硬件综合评估：在增加硬件时，需充分评估其兼容性和性能指标。若对某台服务器进行重大改动（例如增加多块硬盘），则需详细核算其最大输出功率是否满足需求，散热性能是否达标，所采用的 RAID 技术类型，以及该技术是否能与其他硬盘的 RAID 完美融合。

数据中心承压能力：应充分考虑 UPS 的供电能力和精密空调系统的恒温恒湿能力。

服务频率：服务期内按需开展。

服务成果：《服务器扩容服务记录》

3.3.4.网络交换机、路由器、防火墙运维需求

保障网络基础设施的稳定与安全运行，对交换机、路由器及防火墙的精心维护不可或缺。机房内配备了核心交换机两台、交换机共计 24 台、防火墙 6 台以及路由器 3 台，共同构建起坚实的网络架构。

供应商需构建一套全面而完善的网络设备维护体系，涵盖定期巡检、软硬件状态监控、预防性维护保养、安全策略更新与设备升级等多个维度。此外，供应商还应强化人员培训与技术支撑力度，确保网络设备能够持续安全、稳定地运行，为采购人的各项业务活动提供坚实可靠的网络保障。

3.3.4.1.巡检服务

服务需求：

1、设备环境检查：

设备正常运行的前提是其运行环境正常。

设备摆放位置要合理、牢固，应置于通风、干燥的环境，且放置位置要平整，

周围不得堆积杂物。

机房温度状况：机房温度应为0℃～40℃，机房湿度状况：机房湿度应为5%RH～90%RH。

机房内空调运行是否正常：空调应可持续稳定运行，使机房的温度和湿度保持在设备规定的范围内。

清洁状况：要注意防尘网的清洁状况，及时进行清洗或更换，以免影响机柜门及风扇框的通风、散热。设备本身不应有明显灰尘附着。

接地方式及接地电阻是否符合要求，电源连接是否正常可靠，供电系统是否正常。

2、设备基本信息检查：

设备运行的版本：单板PCB版本号、软件版本号是否与要求相符。

检查补丁信息：补丁文件必须与实际要求一致，建议加载该产品版本对应的最新补丁文件。补丁必须已经生效，即补丁的总数量和正在运行的补丁数量一致。

检查系统时间与配置的正确性以及是否保存生效。

运行检查：包括硬件设备以及软件运行状态以及日志的检查。

服务频率：服务期内开展，1次/月，共12次。

服务成果：《网络交换机、路由器、防火墙巡检报告》

3.3.4.2. 故障排除与应急响应

服务需求：在网络设备维护中，负责故障排除及应急响应。对于巡检中发现的故障或用户反馈的故障，需迅速处理，以最大程度减少对服务器运行的影响。一旦发现问题，应立即着手解决，并及时上报。在操作过程中，需确保不影响单位系统的正常运行。若需对设备进行操作，必须按照既定流程完成上报审批。对于紧急故障，提供8小时内上门服务。

服务频率：服务期内按需开展。

服务成果：《网络交换机、路由器、防火墙故障排除与应急响应报告》

3.3.4.3. 备件服务

服务需求：供应商需提供易耗件及备件的更换服务，保障网络的稳定运行。若配件出现老化或损坏，若有备件库存，将立即进行更换；若无备件，供应商应负责修复后及时更换。

服务频率：服务期内按需开展。

服务成果：《网络交换机、路由器、防火墙备品备件清单》

3.4. 视频会议系统运维需求

主要服务内容：

（1）公园管理中心和所属 15 家基层单位的视频会议系统正常会议召开。

（2）公园管理中心与市委市政府之间电视电话会议召开。

（3）公园管理中心与北京市应急管理局、北京园林绿化局之间电视电话会议召开。

具体工作需求：

运维服务的具体工作是为公园管理中心及其所属各单位提供远程技术支持、现场服务、定期巡检、故障处理、突发事件处理、后期培训、提供备品备件等内容。

序号	服务内容	描　　述
1	视频会议支持	针对公园内部软硬件会议，以及市政府会议，市政府加密会议提供会前准备，会中人员支持和会后总结工作还包括市园林绿化局的视频会议。
2	巡检及检修	4 个中心会场 12 次定期巡检以及 15 个直属单位分会场，4 次定期巡检，以及不定期故障排查。
3	中心主会场优化	对中心的主会场的多媒体系统做定期优化调整，确保主会场的会议效果。
4	备品备件	提供相关设备的备品备件，系统出现故障后，能够第一时间以换代修，并长期使用。 所提供的硬件终端必须与现有系统兼容，且为国产品牌。
5	应急处理	在国庆、春节、寒假、暑假等游园高峰时间段，要提供主会场以及各分会场的视频会议应急处理预案，能够确保会议系统正常工作。
6	培　训	各园进行视频会议相关培训 1 次

维保服务要求：

供应商需针对会议室的视频会议系统、视频显示系统、集中控制系统、会议

发言系统、扩声系统、视频切换系统、图像采集系统等开展项目维保服务，具体设备如下：

序号	名称	型号和规格	数量
1	录播系统	威泰视讯	1 台
2	录播系统企业级硬盘	希捷 ES 企业级	2 块
3	多点 MCU	威泰视讯 Meta 2080HD	1 台
4	高清视频会议终端	威泰视讯 VHD	17 台
5	高清视频会议摄像头	威泰视讯 VCM	35 台
6	主扬声器	EAW	34 只
7	吸顶辅助音箱	EXTRON	12 只
8	数字功放	POWERSOFT	17 台
9	辅助功放	高峰	1 台
10	调音台	百威	17 台
11	数字音频处理器	EXTRON	1 台
12	均衡器	百威	1 台
13	反馈抑制器	百威	16 台
13	时序电源控制器	SKD	16 套
15	无线话筒	舒尔	4 套
16	高清投影幕（120”）	DNP 正投硬屏 120”	2 套
17	高清投影幕（100”）	DNP 正投硬屏 100”	13 套
18	视频矩阵	快捷	16 台
19	投影机	富可视	8 台
20	会议主机	快捷 CR-M4101	17 台
21	主席单元	快捷	16 台
22	代表单元	快捷	45 台
23	主席单元线控器	快捷	56 台
24	代表单元线控器	快捷	56 台
25	中控控制主机	快捷 CR-PGMII	2 台
26	无线彩色触摸屏	快捷	2 台

27	红外发射棒	快捷	2 条
28	单向无线接收器	快捷	2 台
29	电源控制器	快捷	2 台
30	音量控制器	快捷	2 台
31	调光器	快捷	1 台
32	RGB 矩阵	快捷	2 台
33	AV 矩阵	快捷	2 台
34	控制软件与编程	快捷	2 套
35	UPS	山特 ARRAY A 4KVA	1 台
36	视频会议应用软件	中信国安视频会议系统 V1.2	1 套
37	软件视频会议服务器	HP 服务器	1 台
38	肩扛式高清摄像机	SONY	2 台
39	高清视频会议终端	中创	15 台
40	全彩显示屏	蓝普视讯	11.06 ㎡
41	视频控制器	蓝普视讯	2 台
42	视频处理器	蓝普视讯	1 台
43	配电柜	蓝普视讯	1 套
44	分配器	宽博	1 台
45	信号延长器	宽博	3 套
46	高清视频会议终端	华为 TE40	2 套
47	会场音箱	GONSIN	4 台
48	功放	GONSIN	2 台
49	会议系统主机	台电 HCS-4100MC/52	1 台
50	会议系统主席单元	台电	1 台
51	会议系统代表单元	台电	6 台
52	无线麦克风	GONSIN	2 套
53	PPT 课件遥控翻页笔	得力	2 套
54	无线会议系统主机	台电 HCS-5300MB/80	1 台
55	无线会议主席单元	台电	1 台

56	无线会议代表单元	台电	13 台
57	电池组	台电	14 套
58	充电箱	台电	2 台
59	音频处理器	GONSIN GX-DSP1013	1 台
60	电源时序器	GONSIN	1 台
61	控制主机	快捷 CR-PGMIII	1 台
62	电源控制器	快捷	1 台
63	控制终端	快捷	1 台
64	双屏移动车	NB	1 套
65	调音台	RATTOP	1 台
66	鹅颈式会议 话筒	SHURE	1 台
67	摄像机	SONY	1 套
68	会场主音箱	GONSIN	2 只
69	功放	GONSIN	1 台
70	监听音箱	RATTOP	1 只
71	路由器	华为	2 台
72	高清模块化 矩阵	宽博	1 套
73	无线会议代表单元	台电	2 台
74	地插	金视	11 套
75	无线会议代表 单元	台电	4 台
76	电池组	台电	4 套
77	无线投屏	BJB	1 套
78	高清视频会议终端	华为 BOX-300	3 套
79	会场监控系统	海康威视	3 套
80	高清混合矩阵机箱	KENSENCE S-Mix-E88	1 台
81	HDMI 输入板卡	KENSENCE	2 块
82	网络输入板卡	KENSENCE	2 块
83	网络发送器	KENSENCE	2 台
84	HDMI 输出板卡	KENSENCE	2 块

85	网络输出板卡	KENSENCE	2 块
86	网络接收器	KENSENCE	4 台
87	多点 MCU	中创 UCM-2000	1 台

运维服务需求：

1. 建立服务目录

供应商按照服务目录的要求向采购人提供服务。合同生效后，供应商应根据实际服务内容，按照采购人要求，对服务目录进行持续补充和完善。

2. 运维资产管理

供应商指定专人，按采购人的要求向采购人提供运维相关文档、资产资料，在发生变更时，及时更新相关文档，使用纸质或电子版更新文档发送到采购人项目负责人确认和备案。

3. 故障维修服务

①系统出现故障时，系统恢复时间不得超过 24 小时；

②当设备出现故障时，供应商应进行免费维修，确保系统正常运行；

③供应商应保证对运维外包对象的维护质量达到设备正常工作的质量要求，在运维外包协议执行期间，供应商维修质量无法达到上述要求，经双方确认后，采购人有权中止运维外包协议或对运维外包范围及数量进行调整。

4. 巡检服务

（1）北京市公园管理中心机关视频会议系统

供应商应每月对北京市公园管理中心机关视频会议系统进行现场巡检，每季度对公园管理中心所属各单位进行现场巡检，在巡检之前，供应商应提出巡检计划和时间安排，经采购人同意后配合巡检。

①供应商应建立现场巡检登记记录，将巡检中发现的隐患及相应的解决办法，以书面方式提交采购人。

②供应商在巡检过程中，发现不能在现场解决的问题，应在三个工作日内给出解决的方案并以予解决。

③巡检内容包括：提供周期性例行巡检、设备清洁和维护保养

④供应商应对北京市公园管理中心视频会议系统开展巡检与维护工作，进行检查、维护，并做好检查记录，并对检查结果进行分析，将报告提交采购人相关

负责人。

（2）分会场系统巡检与设备维护

固定巡检时间段在3/6/9/12月底，不固定巡检写明时间对分会场设备开展巡检与维护工作，进行检查、维护，并做好检查记录，并对检查结果进行分析，将报告提交采购人相关负责人。

（3）日常保障

①提供在北京市公园管理中心视频会议、市政府视频会议、其他会议的日常保障工作。

②每日查看核心设备的运行状况，包括但不限于日常监控、健康检查、数据备份、设备重启等工作。

（4）重要时期、重大活动保障

①供应商需提供以下4种级别的保障方案:

国家级：两会、在京举行的重大活动、重大国际会议等。

市级：北京市两会、北京市重大活动等。

公园管理中心：重大会议、演练活动等。

重大节假日：元旦、春节、清明节、五一、端午、中秋、国庆节等。

②为确保重大活动顺利完成，供应商须派专人到现场进行保障，并提供备品备件。

（5）汛期、灾害预警、突发事件保障

在接到暴雨、暴雪等极端天气预警和突发事件应急保障的通知后进行应急通信系统的保障。供应商需提供保障方案

（6）应急支撑服务

根据北京市公园管理中心视频会议系统的构成和使用编制应急预案，每年进行两次相应的模拟演练，使相关方熟悉应急响应流程，提高对事件的响应能力；同时，验证预案正确性和适用性，并进行完善

（7）系统除尘

每年对北京市公园管理中心视频会议系统进行一次除尘。

（8）远程支持服务

供应商负责设立技术支持团队，为市、下属单位两级提供全年365天7×24

小时远程电话支持服务。

（9）系统优化服务

针对北京市公园管理中心视频会议系统设备的运行情况，提出系统优化及参数设置等方面的合理化建议。

（10）培训服务

制定年度培训计划并编制培训材料，对北京市公园管理中心视频会议系统操作人员、下属分会场操作人员进行现场培训。

供应商定期提供视频会议系统有关产品知识、操作手册、设备运行维护经验、展览会信息、技术文档等资料，并应提供 WEB、FTP 等方式，保证资料方便共享。

（11）运维服务管理

本项目的运维服务人员按采购人要求参与运维服务知识库建设与维护、运维管理体系建设与改进（服务制度、流程、规范等）和运维绩效考核完善与优化等相关工作。

运维服务要求：

（1）服务概述

通过定期巡检、技术指导和咨询服务、故障检修、设备维护等方式，对系统软硬件设备进行维护，对系统故障进行判定并提出解决方案，对系统运行情况进行检查及如实记录，保证系统高效、正常运行。

（2）服务内容

①定期巡检服务：要求供应商派遣专职系统巡检人员，对系统终端用户的软硬件环境、网络环境、设备运行状态等项目进行巡查、检测。每月度运维工程师到中心进行一次常规巡检、所属各单位分会场现场每季度进行一次常规巡检；

每次巡检需填写巡检记录并提交采购人确认。

②设备保修服务：发生故障的设备，要求运维和巡检人员联系设备厂家进行及时维修，并提供易损备件支持。

③确保视频会议终端用户设备的正常使用。

④固件升级服务：在运行维护期间，对系统相关厂商发布的升级要求或补丁程序，供应商承担系统运行环境的固件升级服务，包括操作系统、数据库产品等软件环境的升级和补丁打包，以及终端硬件设备的零部件升级、固件升级等。

服务范围：北京市公园管理中心纳入本次运维范围，分别是北京市公园管理

中心视频会议系统、市委市政府高清视频会议系统、市党政机关加密视频会议系统、市应急管理局视频会议系统及市园林绿化局视频会议系统，共5套会议系统7个多媒体会议室，具体分布情况如下：

序号	名称	位置	主要系统
1	211会议室	2层	无纸化显示系统、会议发言系统、扩声系统、集中控制系统、视频会议系统、视频切换系统、视频显示系统。
2	212会议室	2层	视频会议系统及电视显示设备。
3	二层多功能厅	2层	视频显示系统、扩声系统、会议发言系统、视频系统，集中控制系统。
4	308会议室	3层	无纸化显示系统、会议发言系统、扩声系统、视频会议系统、视频系统、视频显示系统。
5	312会议室	3层	大屏显示系统、会议发言系统、扩声系统、集中控制系统、视频会议系统、图像采集系统、视频切换系统。
6	313会议室	3层	视频会议系统及电视显示设备。
7	一层指挥中心	1层	视频会议系统及电视显示设备。

4. 服务质量管理要求

4.1. 项目团队要求

供应商应为本项目组建稳定的、专业的、独立的服务团队，须在北京设立专门的服务机构，专门负责本项目的安全服务工作。供应商应拥有网络安全方面专业的项目专家，能够及时关注网络及安全设备技术的发展，跟踪最新的网络和安全设备发现的问题或缺陷，搜集整理安全状态、设备漏洞信息、系统补丁信息、

病毒信息等。

项目团队必须配备如下几类人员：项目经理、视频会议系统专项运维人员、驻场工程师及其他服务人员。

其中项目经理须具备 5 年以上工作经验，并同时具备 CISP、信息系统项目管理师（高级）。

除项目经理外，本项目至少配备视频会议系统专项运维人员 3 名，应为从事通信、自动化或音视频相关专业毕业，两年以上相关专业运维经验的工程师，技术能力和经验均可胜任维保及技术支持工作。维护人员须熟悉各单位及会议中心会场系统的工作原理及故障排除方法，对场地、房间的线路走向和设备布置熟练掌握、技术精湛，且态度诚恳，有较强的政治、责任、服务意识，和协调工作的能力。

除项目经理外，供应商应为本项目配备专职安全人员提供安全运维服务，并提供一名专职驻场工程师提供 5×8 安全驻场服务。

服务团队人员应严格遵守采购人的各项规章制度和管理规定，爱岗敬业，不得擅离职守或做与工作无关的事情，能够与客户进行很好的沟通，具有很强的工作责任心和客户服务意识；

4.2. 项目管理要求

供应商应提供详细的项目实施工作计划，明确工作内容以及工作进度安排，制订并遵循安全服务标准化规程。供应商在服务过程中应严格按照相关安全标准，针对服务的各个环节，有专门的项目质量管理保障，包括完善的项目实施流程、实施文档模版和质量记录文档。

4.3. 售后服务要求

供应商应拥有一只稳定的服务保障队伍，并具有较强的技术保障实力，遇到突发情况时能够及时解决问题；服务团队有明确分工和侧重点，基本人员均掌握一般的安全服务方法并能解决常见设备的故障问题；具备提供 7*24 小时应急响应服务能力，针对设备出现的突发故障或问题，在 2 小时到达现场。

4.4. 保密要求

供应商应严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道

德，服从采购人的管理，严格遵守采购人的保密规定和工作制度，并承担相应的保密责任。

所有参与本项目的服务人员，都必须签订《保密承诺书》。供应商负责对《保密承诺书》归档保管，接受采购人检查。供应商要对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向采购人报告。

供应商应自觉接受采购人的安全保密监督和管理，如违反安全保密条款，采购人将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对供应商泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还将依法承担相应的民事责任。

4.5.项目验收

本项目在服务完毕之日起15个工作日内，供应商提供所有服务期内产生的纸质文档和电子文档，并向采购人提出最终验收申请，采购人组织项目验收工作。

合同附件三：

保 密 协 议

甲乙双方就“信息化运维费采购 01 包 信息化基础运维”项目签订合同，甲方委托乙方提供运维服务(以下简称“本委托事项”)，为保障甲方商业秘密不因本委托事项而泄露以致对甲方造成损失，甲、乙双方就在本委托事项过程中，以及完成后乙方的保密职责达成如下协议条款：

一、保密责任的范围

本委托事项涉及保密内容主要是甲乙双方在订立合同过程中，知悉的商业秘密、版权、专利等（无论合同是否成立，不得泄露或者不正当地使用、复制、扩散)。乙方为甲方提供的服务内容中涉及设备配置、密码等方面的商业秘密。包括但不限于：

基础化运维的运维工作中，硬件部分所涉及到数据和任何记录，包括但不限于：巡检报告、设备清单、节日保障相关记录文件、故障处理相关文件、内部管理文件等。

基础化运维的运维工作中，软件部分所涉及到数据和任何记录，包括但不限于：账户管理数据、经营数据、客户信息数据、专有设计、功能开发、上线相关数据和记录以及涉及到的所有保密性质的材料、文件等。

基础化运维的运维工作中，安全部分所涉及到数据和任何记录，包括但不限于：安全保障产生的数据（包括数据安全、系统安全、应急安全)、等。

基础化运维的运维工作中，产生的其他业务所涉及到数据和任何

记录。

二、双方承诺

甲方提供本委托事项所需的资料和信息，并对所提供资料和信息的真实性和准确性做出承诺。

乙方承诺根据甲方提供资料和信息按照国家有关法律法规执行本委托业务，乙方应当向甲方或甲方指定方披露按照《民法典》等法律法规规定的本次委托事项中的合适、可行方案及相关信息。

三、双方责任

甲乙双方互为保密资料的甲方和乙方，负有保密义务，承担保密责任。

乙方未经甲方书面同意不得向第三方（包括新闻界人士）公开、披露、透露或泄露任何保密资料或以其他方式使用保密资料。乙方也须促使其代表不向第三方（包括新闻界人士）公开、披露、透露或泄露任何保密资料或以其它方式使用保密资料。除非披露、公开或利用保密资料是乙方从事或开展合作项目工作在通常情况下应承担的义务（包括乙方今后依法律或合同应承担的义务）适当所需的。

乙方须把保密资料的接触范围严格限制在因本协议规定目的而需接触保密资料的工作人员/雇员范围内。

除经过双方书面同意而必要进行披露外，乙方不得将含有甲方或其代表披露的保密资料复印或复制或者有意无意地提供给他人。

如果合作项目不再继续进行或其中一方因故退出此项目，经甲方在任何时候提出书面要求，乙方应当、并应促使其代表在五个工作日内销毁或向甲方返还其占有的或控制的全部保密资料以及包含或体现了保密资料的全部文件和其它材料并连同全部副本。但是在不违反

本协议其它条款的条件下，乙方可仅为本协议第四条保密资料的保存和使用目的，保留上述文件或材料的复制件一份。

乙方将以并应促使其代表以不低于其对自己拥有的类似资料的保密程度来对待甲方向其披露的保密资料，但在任何情况下，对保密资料的保密措施都不能低于合理程度。

四、保密资料的保存和使用

乙方有权保存必要的保密资料，以便在履行其在合作项目工作中所承担的法律、规章与义务时使用该等保密资料。

乙方有权使用保密资料对任何针对乙方或其代表的与本协议项目及其事务相关的索赔、诉讼、司法程序及指控进行抗辩，或者对与本协议项目及其事务相关的传唤、传票或其他法律程序做出答复。

乙方在书面通知甲方并将披露的复印件抄送甲方后，可根据需要在提交任何市、省、中央或其他对乙方有管辖权或声称对乙方有管辖权的监管团体的任何报告、声明或证明中披露保密资料。

根据国家有关法律，因国家司法部门和政府机构需调阅乙方的公司档案或要求乙方做出必要说明的，如涉及商业秘密、并已书面通知甲方的，则不在本保密协议约定的乙方保密义务之内。

五、　违约责任

任何一方违反本协议所规定的保密义务，承担由此引起的责任。违约方应按服务费的30%支付违约金，金额为人民币558,360.00元（大写：人民币伍拾伍万捌仟叁佰陆拾元整）。

六、适用法律和争议解决

本协议的所有方面均适用中华人民共和国法律进行解释并受其约束。本约定书履行地为甲方所在地，因本协议所引起的任何纠纷或争议，双方选择提交至甲方指定仲裁委员会进行仲裁。

合同附件四：

合同履约考核表

经办部门		合同编号	
合同名称	信息化运维费政府采购合同 包号/分包名称：01 包/信息化基础运维	合同金额	1,861,200.00 元
合同有效期	1 年	服务商名称	北京数字认证股份有限公司

考核内容	考核指标	分数	得分	考核标准	扣分原因
合同管理	在规定时间内完成项目所需各类手续、文件的办理及提交且提交内容齐全/完整。	5		手续准备不齐全、有缺失或出现后补情况扣 1 分；	
				无故延误提交，延误三个工作日及以上扣 2 分；	
	按合同约定，在服务期限内项目计划任务完成度达 100%及以上。	20		按照服务计划，无故延误进度，每延误一个工作日扣 1 分；	
				服务到期，项目计划任务完成度达 99%-95%扣 5 分；	
				服务到期，项目计划任务完成度达 94%-50%以下扣 10 分；	
				服务到期，项目计划任务完成度达 49%-0%该项不得分；	
	运维保障、技术支持等服务效果达到合同约定且符合预期。	10		效果一般扣 1 分；	
				效果较差扣 2 分；	
	按照合同价款约定，及时提供等额、有效、合法结算票据。	5		未在规定时间内提供，延误一个工作日扣 1 分（特殊情况经甲方同意除外）；	
				未提供等额、有效、合法结算票据该项不得分；	

服务管理	项目执行中，未出现因设计遗漏、操作失误等问题导致严重或一般故障/事故。	10		出现一般事故，造成影响及损失扣 5 分； 出现严重事故，造成影响或损失该项不得分；	
	提供详细完整的运维、服务记录（包括但不限于服务方案、工单、报表等）。	10		提供的文档资料不够完整/详细扣 2 分； 未提供相关文档资料该项不得分；	
	服务期满前提供详细完整的服务报告（包括但不限于周报、月报、季报、年报等）。	10		提供的报告不够完整、详细扣 2 分； 未按要求提供服务报告该项不得分；	
	对于服务内容中衍生的常规问题能及时合理安排技术人员进行处理，且处理得当。	5		基本能较快响应，问题解决速度较快扣 1 分； 响应速度超出约定时限，问题解决速度慢扣 2 分；	
	对于突发、紧急事件能在 30 分钟以内响应。	5		基本在 30 分钟以上，60 分钟以内响应扣 1 分； 基本在 60 分钟以上响应或无人响应该项不得分；	
	项目过程中，保密措施得当，效果良好。	5		保密工作落实一般扣 1 分； 保密工作落实较差扣 2 分； 无保密措施或出现泄密等重大过失该项不得分；	
人员管理	项目执行期内未擅自更换项目、技术等主要负责人（特殊情况经甲方同意除外）。	5		未经甲方同意，擅自更换项目、技术等主要负责人，造成对接有脱钩、服务有延误等情况扣 2 分； 未经甲方同意，频繁发生项目、技术等主要负责人更换，且人员管理混乱，造成对接有脱钩、服务有延误等情况该项不得分；	
	对本项目范围内的**对内**关系协调机制完善，沟通顺畅，以保证各项工作进行顺利。	5		经常联系不到项目对接联系人扣 1 分； 项目对接联系人对于业务理解、沟通协调能力不足扣 2	

				分；	
	对本项目范围内的**对外**关系协调机制完善，沟通顺畅，以保证各项工作进行顺利。	5		由于协调不到位影响到工作进度，每次扣 1 分； 由于协调不到位造成事故、停工或其他恶劣影响，每次扣 2 分；	
	总分	100			
经办部门审批意见： 考核结果：□优秀 □良好 □合格 □不合格 部门负责人签字： 时间：					
服务商代表签字确认： 时间：					

说明：

1、按“优良”（90-100 分）、“良好”（75-89 分）、“合格”（60-74 分）、“不合格”（59 分及以下）四个等级划分；

合同附件五：

奖 惩 措 施

甲乙双方就“信息化运维费政府采购合同 01包 信息化基础运维”项目签订合同，甲方委托乙方提供运维服务，为保证北京市公园管理中心等9个业务信息系统，中心音视频运维服务项目在运维过程中稳定运行特制定奖惩措施。该措施更好地明确了奖惩的依据、标准、权限及程序，形成良好的奖惩机制，提高运维团队与个人的主观能动性。

一、处罚措施

对于北京市公园管理中心等9个业务信息系统，音视频运维服务项目所出现的各级运维故障，如果运维故障的主要原因由人为工作疏忽/失误所导致，参照以下故障处罚标准对个人和项目组进行相关惩处，任何运维故障，要及时通报相关领导或相关处理人员，对于延报、瞒报故障者，将从严处罚。

（一）故障非常严重

1. 网络系统完全停止工作/停机（且0.5小时内未电话响应、4小时内未上门）

2. 关键业务不能完成进行工作（且0.5小时内未电话响应、4小时内未上门）

3. 工作完全停止（且0.5小时内未电话响应、4小时内未上门）

4. 音视频设备停止工作/停机（且0.5小时内未电话响应、4小时内未上门）

5. 视频会议系统不能正常运行（且0.5小时内未电话响应、4小时内未上门）

6.音视频系统工作完全停止（且0.5小时内未电话响应、4小时内未上门）

（二）故障严重

1. 系统不能连续工作，有效工作时间<70%（且0.5小时内未电话响应、4小时内未完成故障排查）

2. 业务无法正常工作（且0.5小时内未电话响应、4小时内未完成故障排查）

3. 系统报告出现错误或警告（且0.5小时内未电话响应、4小时内未完成故障排查）

4.音视频系统不能连续工作，有效工作时间<70%（且0.5小时内未电话响应、4小时内未完成故障排查）

5. 音视频系统无法正常工作（且0.5小时内未电话响应、4小时内未完成故障排查）

6. 音视频系统报告出现错误或警告（且0.5小时内未电话响应、4小时内未完成故障排查）

7. 中心及各下属公园视频会议终端出现故障

4. 用户端出现错误

（三）故障紧急

1. 导致系统或业务性能大幅度降级的问题，会影响服务质量或严重威胁网络操作人员的控制及运行效率。（且0.5小时内未电话响应、8小时内未完成故障排查）

2. 整个网络均运行质量下降，严重影响操作人员正常运行。（且0.5小时内未电话响应、8小时内未完成故障排查）

3. 网络管理软件的主要特性无法运行而且很难找到变通方法。（且0.5小时内未电话响应、8小时内未完成故障排查）

4.导致音视频系统无法使用的问题,严重影响中心会议无法正常召开使用。(且0.5小时内未电话响应、8小时内未完成故障排查)

5.视频会议系统出现视频终端故障,严重影响中心与下属各公园无法参加视频会议召开。(且0.5小时内未电话响应、8小时内未完成故障排查)

6.视频会议终端的主要功能无法运行而且很难找到变通方法。(且0.5小时内未电话响应、8小时内未完成故障排查)

(四)故障一般

1. 影响系统运行、维护和管理且要求立即采取措施的故障。(且2小时内未电话响应、12小时内未完成故障排查)

2. 对系统性能、客户及其运营的影响较小。(且2小时内未电话响应、12小时内未完成故障排查)

甲方视情节严重程度对乙方进行通报批评,按故障的严重程度对乙方进行罚款:

1、故障非常严重:每次罚金2000元;

2、故障严重:每次罚金1500元;

3、故障紧急:每次罚金1000元;

4、故障一般:每次罚金500元;

(五)合同履约考核结果

在项目期满后,按照合同履约考核结果进行相应比例支付第三笔费用(即合同金额的25%):

(1)合同履约情况优秀的,第三笔费用全额支付。

(2)合同履约情况良好的,第三笔费用支付合同总金额的20%,核减5%。

(3)合同履约情况合格的,第三笔费用支付合同总金额的15%,

核减 10%。

（4）合同履约情况不合格的，第三笔费用全部核减。

如出现上述需要对乙方进行缴纳罚金及核减费用的情况，甲方将以双方签字盖章的确认单作为相关处理依据。

二、奖励措施

运维团队奖励:在规定的运维期内，做到满足运维总体要求,获得用户的认可,对整个运维团队给予嘉奖通报、授予优秀运维团体荣誉，颁发荣誉证书。

个人奖励：在规定的运维期内，做到满足运维总体要求，个人工作努力、业务纯熟，给予嘉奖，授予优秀个人荣誉，颁发荣誉证书。