# 北京市残疾人服务示范中心

# 网络安全运维项目

# 合同书

| | |
|---|---|
| 甲方 | ：北京市残疾人服务示范中心 |
| 乙方 | ：首都信息科技发展有限公司 |
| 日期 | ：2026 年 4 月 13 日 |

# 项目合同书

**甲方：北京市残疾人服务示范中心**

**法定代表人：杨志强**

**统一社会信用代码：12110000764202833M**

**住所地：北京市丰台区莲花池南里 23 号**

**电话：010-83771817**

**乙方：首都信息科技发展有限公司**

**法定代表人：夏晓清**

**统一社会信用代码：9111010878995031XQ**

**住所地：北京市海淀区知春路 49 号 4 层西部 401 房屋**

**电话：010-88511155**

甲方委托乙方开展北京市残疾人服务示范中心 2026 年度网络安全运维项目（以下简称“项目”），甲乙双方根据《中华人民共和国民法典》及其他法律、行政法规的规定，在平等、自愿、公开、诚实信用的基础上友好协商，签订本合同，以资共同遵守。

**第一条 委托事项**

乙方应按照合同所列内容组织北京市残疾人服务示范中心 2026 年度网络安全运维项目的实施。

具体需求如下：

1、服务对象： 北京市残疾人服务示范中心 。

2、服务内容： 具体服务内容详见《运维服务内容》（附件 1） 。

3、服务目标： 将“以客户服务为中心，不断提高服务满意度”作为服务管理目标，

通过制定完备的技术服务流程和借助富有经验的技术支持与服务队伍，确保示范中心办公网络高效、安全、稳定、可靠地运行。制定以“客户满意度”为核心的服务目标，服务满意度：大于 90%，网络系统可用性：大于 99%，响应及时率：大于 95%，常规运维任务完成率：大于 99%。

4、服务要求（质量、指标）：具体服务要求详见《运维服务方案》（附件 2）。

5、验收方式及内容：项目结项后，乙方向甲方提交工作周报、月报、记录单等服务过程文件，甲方按照附件 1《运维服务内容》和附件 2《运维服务方案》的要求，对乙方服务内容进行验收，并出具《项目验收单》。

**第二条 服务期限及地点**

1、服务期限：2026 年 4 月 13 日至 2027 年 4 月 12 日

2、服务地点为：北京市丰台区莲花池南里 23 号（汇爱大厦）。

**第三条 项目经费及支付方式**

1、本项目经费共计¥ 282,900.00 元（大写：人民币贰拾捌万贰仟玖佰元整）。

2、甲方应于合同生效后 20 个工作日内，向乙方指定账户支付项目经费总额的 70 %，即：¥ 198,030.00 元（大写：人民币壹拾玖万捌仟零叁拾元整）；

3、项目结项通过甲方验收合格后 7 个工作日内，甲方向乙方指定账户支付项目经费总额的 30 %，即¥: 84,870.00 元（大写：人民币捌万肆仟捌佰柒拾元整）；

4、甲方付款后，乙方应向甲方出具合法有效的等额增值税专用发票；

5、乙方指定账户信息如下：

户名：首都信息科技发展有限公司

开户行：中国银行北京市分行

账号： 331156006031

**第四条 履约保证金**

本项目不涉及。

**第五条 甲方的权利及义务**

1、积极配合乙方开展项目，为乙方提供必要的工作便利。

2、对乙方的运维服务方案提出改进意见。

3、监督乙方按照运维服务方案开展项目。

4、按照合同约定，甲方在乙方按时保质的履行本合同项下约定的服务内容基础上，及时且足额地向乙方支付项目经费。

5、本合同下的一切成果归甲方所有。

**第六条 乙方的权利及义务**

1、按照合同期限完成项目工作。

2、乙方派遣品行端正、责任心强、具有良好职业道德，且符合岗位要求的工作人员开展工作，并确保与所派工作人员具有正式、合法且有效的劳动合同关系。

3、乙方安排的工作人员应具备良好的沟通协调能力，确保工作的连续性。

4、定期与甲方沟通，使甲方了解乙方工作人员的工作情况，对不能胜任岗位要求或不服从管理的工作人员，乙方应在 3 日内予以更换；乙方调换工作人员应提前告知甲方，并获甲方同意后才能调换。

5、乙方应对所派人员在提供服务过程中造成的一切责任以及因工伤、因病缺勤等后果负责，包括但不限于给甲方造成的直接或间接经济损失、给第三方造成的损失、所派人员工伤、律师费、鉴定费等。

6、主动就项目的开展和实施征求甲方意见，根据甲方的意见持续调整项目的运维服务方案，保证项目取得预期效益。

7、保证向甲方提交全部开展和实施项目期间所取的成果，且任何第三方不会就乙方

提交的全部成果向甲方主张任何权利。

8、保证开展和实施本项目不会侵犯其他任何第三方的任何权利或者违反国家法律法规规定。

9、未经甲方书面同意，乙方不得将本合同项下的工作项目全部或部分转让给任何第三方实施。

**第七条 保密**

1、甲乙双方应当对签订和履行本合同而获得的与下列各项有关的信息，负有严格的保密义务：

（1）本合同的各项条款。

（2）有关本合同的谈判。

（3）合同乙方提供的涉及提供方专属的或保密的信息和数据。

2、仅在下列情况下，甲乙双方可披露上述信息：

（1）依法律、法规的规定。

（2）依任何有管辖权的政府部门或监管机构或协会的要求。

（3）并非由于任何一方过错而众所周知的信息。

（4）甲乙双方事先达成书面认可。

3、本条款的适用不因合同的终止而失效。

**第八条 违约责任**

1、任何一方违反本合同项下约定的事项，均视为违约，作出违约行为的相对方有权单方解除本合同，并有权要求违约方赔偿因此遭受的一切损失，包括但不限于直接损失、间接损失和追偿损失而产生的律师费等全部费用。

2、乙方不能按合同约定完成项目，甲方有权单方终止合同，乙方应当自合同约定的项目期限届满之日起 30 日内归还甲方已支付的全部项目经费。

3、若乙方迟延履行上述返还义务，每逾期一日，应按照乙方应当返还的全部项目经费的每日 0.5 %向甲方支付违约金，直至乙方全额返还相关费用及支付违约金之日止。

4、乙方在为甲方服务时获得的数据和形成的报告等成果全部归甲方所有，未经甲方许可，乙方及其乙方人员不得以任何方式使用，也不得出于任何目的向第三方披露或许可第三方使用，否则乙方需按照本合同总金额的 20%承担违约责任。

**第九条 不可抗力**

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。

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，在事故发生后 7 日内，将有关部门出具的证明文件送达另一方。

3、不可抗力使合同的某些内容有变更必要的，双方应通过协商在未受事故影响一方收到书面通知后 7 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。

**第十条 合同的生效、变更和终止**

1、本合同经双方法定代表人或授权代表签字并加盖公章或合同专用章后生效。

2、如双方对本合同内容进行变更或补充，应共同协商，签订补充协议。补充协议作为本合同的附件，与本合同具有同等法律效力，补充协议与本协议不一致的，以补充协议为准。

3、除本合同项下的相关约定外，出现下列情况之一，本合同应当终止：

（1）经甲乙双方协商终止；

（2）本合同约定项目完结且经甲方验收合格。

**第十一条 争议解决**

1、在合同履行过程中发生争议的，双方首先应当友好协商解决，协商不成的，可向

丰台区人民法院提起诉讼。

2、除争议事项外，乙方应继续行使其剩余的相关权利，履行本合同项下的其他义务。

**第十二条 其他**

1、本合同构成甲乙之间就本合同项下事项的全部内容，并取代双方之间此前所有与本协议事项有关的一切讨论（不论是书面或是口头形式）和所有其他文件和协议。

2、双方确定，在本合同有效期内，甲方指定 刘嵩杰 为甲方项目联系人（手机：13911698861，乙方指定 潘雪飞 为乙方项目联系人（手机：13511061806）。乙方变更项目联系人的，应当自变更事项发生之日起 3 日内以书面形式通知甲方，否则所产生的损失由乙方承担。

3、本合同附件包括：《运维服务内容》（附件 1）、《运维服务方案》（附件 2）。合同附件是本合同不可分割的组成部分，与本合同具有同等法律效力。

4、本合同一式 四 份，甲、乙双方各持 两 份，具有同等法律效力。

（以下为合同签署页，无正文）

甲方（盖章）：北京市残疾人服务示范中心

法定代表人或授权代表（签字）：

日期：2026年4月13日

乙方（盖章）：首都信息科技发展有限公司

法定代表人或授权代表（签字）：

日期：2026年4月13日

附件 1

# 运维服务内容

## 一、网络运维服务内容

1. 按照需求制定网络运维服务方案；

2. 网络设备日常每月巡检维护；

3. 网络设备按需优化调整；

4. 网络节点的安装调试、规划，网络线路与墙点的日常维护；

5. 网络及链路故障处理服务；

6. 协助网络运营商对中心机房的网络链路进行故障诊断，积极联络、协调、配合网络运营商解决网络链路的问题。

## 二、安全运维服务内容

1. 安全设备日常每月巡检维护；

2. 安全设备按需优化调整；

3. 从技术层面加强网络安全策略配置，优化网络及安全设备性能，及时进行网络及安全设备安全加固，减少信息安全隐患，提高网络及系统安全防护能力；

4. 掌握楼内网络接入终端网络使用情况，屏蔽不安全的设备和人员接入网络，规范用户接入网络的行为。

## 三、机房运维服务内容

负责中心机房的日常管理工作，包括机房内服务器、网络设备、安全设备定期巡检、故障排查、维护等，机房基础环境的日常巡检及维护，机房人员进出、设备进出管理，以及故障排查和处置。

## 四、会议保障服务内容

1. 保障会议室音、视频正常使用，视频会议通信线路通畅。

2. 会议中全程保障，根据会议需求，适时调节音量，遇到问题及时处理。

3. 完成会议系统、音响系统及显示系统的调试及会议保障工作。

附件 2

# 运维服务方案

## 一、网络运维服务方案

### 1. 网络系统定期巡检

提供中心大楼网络巡检服务，根据中心大楼网络环境制订巡检方案，按计划对所有业务网络的网络设备运行状况进行现场检查，收集设备运行参数，并提供《网络系统巡检报告》。

**（1）服务内容**

首信公司安排网络工程师组织定期现场巡检，及时发现设备问题，保持业务的连续性，并对各设备运行状态、使用情况进行检查，包括：硬件环境、设备CPU、内存状态，端口状态、版本信息、系统日志、升级情况等，并在巡检当日填写巡检记录、提交巡检分析报告（网络巡检3日内提交《网络巡检分析报告》），巡检范围包括网络链路、路由器、交换机、防火墙、安全设备等。

**巡检流程：**

1) 制定巡检计划，用户确认后执行。

2) 工程师出发前电话通知所巡检单位的用户联系人巡检服务时间计划，以便让用户方提前做好相应配合准备；

3) 工程师到达客户现场后，输入登录设备帐号、密码，登录至用户特定巡检设备，作为设备巡检的准备工作。

4) 进入到特定网络设备，进行常规巡检操作：（不同品牌网络设备操作命令会有所差异。）

   a) Show version 查看当前设备 IOS 版本；

   b) Show logging 查看日志；

   c) show processes cpu 查看 CPU 资源使用情况

   d) show processes mem 查看内存资源使用情况

e） show module 查看模块信息；

f） show environment all 查看所有模块温度

g） Show interface 查看端口使用情况；

h） Show tech 查看设备所有信息

5）按巡检报告要求收集必要的信息，包括静态信息和动态信息；

6） 如发现问题，及时处理并告知用户负责人，将问题进行记录；根据收集到的信息填写巡检报告；

7） 网络设备巡检记录完成后，等待用户负责人确认后，退出登录特定设备，网络设备巡检完毕；

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 网络定期巡检服务 | 定期对网络及安全设备进行巡检、及时发现网络运行中出现的隐患，减少网络发生故障概率，保障业务连续性。 | 5 天×8 小时 |
| | | 对核心网络及安全设备每天巡检 1 次，其它网络及安全设备每月巡检 1 次，3 日内提交网络巡检分析报告。 |

**2．运行状态监测**

对中心网络及网络安全设备的运行状态进行监测，每月提交《网络及安全设备运行状态监测报告》，为网络优化、故障甄别、网络安全加固、安全策略优化提供依据。

**（1）服务内容**

通过技术手段，利用网络资源，依靠监控软件，为用户提供整体网络运行状态监控服务，监控对象包括网络光纤、专线链路状态、网络及安全设备资源使用情况、网络流量使用情况，监控系统通过声音报警方式对中断链路进行提示。在发现故障时，可第一时间进行处理，并在最短时间内尽快恢复业务系统正常。

1）对用户网络光纤链路及网络设备运行状态进行实时监控。

2）发现网络中断时，工程师按用户指定的方式及时通知相关人员，并通过服务台系统

进入故障处理流程。

3）定期（每月）备份用户网络监控记录，以对网络问题的追溯分析、网络优化、故障甄别、网络安全加固、安全策略优化提供依据。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 运行状态监测服务 | 根据日常网络运行状态监控信息进行统计、分析，可为网络优化、故障甄别、网络安全加固、安全策略优化提供依据。 | 5 天×8 小时<br>1 次/月 |

**3．网络安全事件综合分析**

利用已建成网络安全系统中各设备所采集的安全事件、安全信息，结合当前最新安全趋势和风险防范要点，以及运行过程中出现的事件，参照信息系统等级保护要求等相关标准，综合分析当前网络的网络安全形势，提出各网络安全优化措施建议。

**（1）服务内容**

网络作为支撑业务运转的基础设施，其安全性直接影响到业务系统稳定性和可靠性。网络系统的安全方案设计与安全优化的需求来自两个途径：一是通过日常维护中发现的问题（包括安全隐患、网络架构等）进行分类、统计、分析，或者经过对现有网络、安全设备运行数据进行采集分析，对网络结构进行调整或改造能够提高网络整体安全性；二是根据业务的不断发展，增加新的业务需求，需要对现有网络安全进行提升，或者对某几个网络业务进行整合、优化，需同步提升整体网络安全性。

首信公司在用户进行网络安全运维服务过程中，通过网络安全设备信息的统计和分析结果，依据电子政务网络的建设要求及规范，详细调研、认真分析。结合网络现状给出网络安全方面的评估建议书，将根据评估结果草拟《网络安全优化建议》及《网络安全整改方案》，在用户认可后负责对网络系统进行安全加固。

网络安全加固分为两种情况进行：

1）首信公司在巡检和维护过程中发现的网络安全问题，将及时向用户提出整改意见，并根据具体情况进行安全加固实施；

2）首信公司接到用户有关安全方面的技术请求，及时响应并进行处理。

安全加固服务流程：

1）首信公司根据用户的要求为网络系统提供安全加固服务，包括厂商公布的软件和配置等。

2）首信公司向用户了解现有的安全策略，并且和用户沟通网络要求的恢复目标。

3）首信公司提供满足要求的安全策略，在用户的认可下，进行安全加固。

4）安全加固的成果需要进行验证和测试。

5）首信公司在巡检过程中做安全加固工作，应在不影响网络的情况下进行。

6）首信公司完成现场网络系统安全加固服务后，填写并提交《网络设备安全加固记录表》。

7）在服务过程中首信公司对用户进行现场讲解。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 网络安全事件综合分析服务 | 根据日常维护、巡检发现的安全隐患，或者用户新增的安全需求，进行分类、统计、分析，并出具网络安全评估结果，在用户认可的情况下实施安全加固操作，从而提高网络的安全性。 | 5 天×8 小时 |

**4．应急救援服务**

当网络发生异常情况时，需 30 分钟内判断故障原因，如遇特殊网络故障，须提供资深网络专家协助对情况进行综合分析解决，必要时须提供非本项目内运维设备、备机等以外的替代设备实现网络恢复。

**（1）服务内容**

首信公司为用户提供应急救援服务，根据用户网络服务质量和业务要求，针对突发事件制定应急救援预案，能够在 30 分钟内判断故障原因，并为应急救援突发事件提供足够的

人力和技术保障，以确保网络系统发生故障或面对意外突发事件时，网络服务能在最短时间内得以恢复以使正常的业务继续进行，将损失降低到最小限度。并根据用户业务外网、业务内网和互联网的重要程度，通过应急救援服务，达到以下目的：

1）建立应对网络应急事件的快速高效、分工明确、责任到人、常备不懈的应急组织及保障体系；

2）建立应对网络应急事件防范、指挥、处置体制和机制，提高处理和解决网络应急事件的响应能力；

3）通过规范网络应急事件的等级分类，确定不同等级应急事件的启动程序，明确运维人员的职责和权利；

4）尽快消除事件影响，尽可能减少事故造成的损失。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 应急救援服务 | 充足的硬件设备和人员储备，满足在突发网络事件发生时，能够在30分钟内定位故障点，并启动应该救援方案，及时、快速的处理网络故障。 | 7天×24小时 |

**5．故障诊断、故障处理**

对于用户网络运行过程中发生的各种故障，首信公司提供现场技术支持服务，确定故障原因、并排除故障。首信公司需要提供每一次的《故障分析及解决报告》。

**（1）服务内容**

根据故障的具体情况，采取必要的服务措施(包括调整)，尽快修复故障，恢复网络系统正常运行。首信公司通过现场服务、电话指导等方式进行故障诊断与处理，并保证满足双方约定服务等级中的处理时限。故障处理流程简述如下：

为提高总体服务质量，实现服务满意度质量目标，首信公司早在2003年就开始了基于ITIL（ILInformation Technology Infrastructure Library）思想提高IT服务质量的探

索和应用。经过多年的摸索和实践，我们已经成功的在网络服务中运用和贯彻了 ITIL 思想，并通过在实际服务工作中部署服务台、事故管理、问题管理、配置管理、变更管理和服务级别管理等 ITIL 核心流程，建立起了专业化、电子化的网络服务体系。

故障管理应用了 ITSM 事件管理思想，确保了故障处理结果符合质量目标要求。在故障处理过程中，要确保在尽可能小地影响客户和用户业务的情况下，快速恢复网络系统业务，从而达到服务级别标准。当多个故障需要同时处理时，必须根据事故所造成的影响、事故的紧急程度、解决事件的难易程度等因素确定事故处理的优先级。如果在协议约定的时间内一线支持无法解决事故，则通过事故升级（Incident Escalation）协调更多的支持人员介入。事故升级（Incident Escalation）的一般程序。一线支持一般指服务台支持工程师，二线支持指现场服务工程师，三线支持指网管工程师，四线支持指第三方服务商。

我们通过过程监督提高故障处理效果。通过网络监控、定期巡检等技术手段，提早对故障点进行定位，为客户提供网络服务支持，从而提高客户的满意度。

1）故障处理时间

通过完整的事故管理流程我们能够做到 30 秒接收故障情况，故障处理响应时间小于 10 分钟，对于需要现场处理的故障，城区用户可在 2 小时内到达现场，郊区用户可在 4 小时内到达现场，并及时向用户申告人员通告故障处理进展情况。

2） 故障通知

故障通知是指是我方主动发现故障的情况下，在网络链路发生持续 5 分钟以上的中断时，在 10 分钟之内通过用户选定的通讯方式及时通知用户，并在确定问题后进入故障处理流程。

首信公司现场工程师使用网络监控平台，辅以桌面声、光报警系统，实时监测网络链路状态，一旦出现链路中断情况，能够及时发现。

3）故障处理服务

a） 现场工程师必须了解用户网络结构、路由协议及管理部分布等基本情况，了解网络系统运行情况及以往所发生过的问题及处理办法；

b） 工程师准备笔记本电脑、故障诊断软件、测试仪等技术服务工具、相关备件、交通工具。

c） 现场工程师根据故障现象对网络系统进行故障分析、测试、诊断，并制定业务

恢复和故障解决技术方案，技术方案经用户批准后，再进行具体实施。

d) 如果确定为系统硬件故障，及时汇报用户，提供备件，首信公司根据需及时更换备件。

e) 在必须进行网络系统重装或重启等影响较大操作时，须经用户批准方可实施。

f) 现场工程师在处理故障后，向用户或负责人解释故障原因和解决方法，并提醒在日常维护中的预防措施。

g) 现场工程师在处理故障后，将撰写《故障分析及解决报告》，并在离开现场前交用户存档，同时由用户用户对现场服务质量给予评价。

h) 故障分析报告

在故障处理运转流程中，每一条故障处理记录都会被记录到事件数据库和问题数据库，可近一步的进行分析并形成报告。

i) 对于电话支持解决的故障，首信公司服务台记录故障处理过程，导入知识库，可为事件分析、问题分析提供依据。

j) 对于现场技术支持解决的故障，现场工程师填写《故障分析及解决报告》，详细记录故障处理过程、原因，并由用户给出服务满意度评价，便于不断提高和改进服务能力。

k) 首信公司按月提交包括故障处理内容的《网络运行维护报告》。

4) 故障等级分类

适用范围：此处故障等级的分类和定义适用于用户网络 IT 服务管理过程中所涉及的所有网络故障。

分级的目的是为根据故障的严重性从而确定对该项事件采取相应的行动优先级别。

用户网络平台发生的网络故障，根据影响范围和程度，共分三个等级。网络平台事件严重性和响应优先级别根据下表进行判断。详见下表：

故障等级分类表：

| **事件等级** | **说明** | **故障处理响应时间** | **影响（判断依据/标准）** | **优先先级** |
|---|---|---|---|---|
| L1 红色 | 重大故障 | 5 分钟 | 【1】全网瘫痪，彻底影响用户正常工作/用 | 高 |

| | | | | |
|---|---|---|---|---|
| | | | 户无法正常工作；<br>【2】核心网络设备/节点无法提供通信服务；<br>【3】业务系统数据传输中断；<br>【4】在重点保障其间（有相关文件依据或领导指定，如安全日历时期、市政府领导参观访问时期），用户发生网络中断； | |
| L2 橙色 | 中级故障 | 30 分钟 | 【1】1 个以上的部门无法提供通信服务；<br>【2】在非重点保障期间，1 个以上的部门连接中断，或者勉强可以使用，但已严重影响用户使用性能，影响大部分终端用户工作； | 中 |
| L3 黄色 | 一般故障 | 60 分钟 | 【1】可以维持正常工作；<br>【2】仅影响一个或个别用户使用； | 低 |

注：响应时间是指在指定时间内开始处理该项事件。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
|---|---|---|
| 故障诊断、故障处理服务 | 建立运维服务体系，通过现场、远程电话技术支持的方式，及时处理用户申报或自动发现的网络故障，并提供每一次故障的《故障分析及解决报告》，保障网络可用性大于 99%。 | 7 天×24 小时电话技术支持，故障处理响时间小于 12 分钟，电话回复时间小于 30 分钟。 |

**6．网络设置、网络管理、策略调整**

对网络设备和安全设备进行日常使用及维护，及时处理网络系统异常。根据网络管理需求，及时更新和调整网络设备和安全设备相关配置策略，并对相关系统配置进行必要备份。

**（1）服务内容**

根据用户网络及业务系统使用需求，由用户提出变更申请，对需要增加、变更的 IP 地

址、VLAN、ACL、路由、安全策略及相关需求进行服务支持，完成后由用户进行业务测试并签字确认。主要配置调整包括：

1）IP 地址的规划管理：

根据用户网络 IP 地址资源，合理规划网络设备互联地址、网络设备 IP 地址段分配、网络设备间 IP 地址路由规划、网络设备管理及维护地址等。我们建议用户 IP 地址的规划应用遵照统一的规划原则，合理分配使用。IP 地址使用不规范的应用要逐渐地修改，避免对业务造成影响。对迁址或合并的管理部 IP 地址必须及时回收，除了删除网络设备的配置数据外，还要建立 IP 地址维护台帐，使 IP 地址资源管理规范化。

2）VLAN 的规划管理：

Vlan 将网络划分为若干子网以方便网络管理，并且使数据限制在本地流动，保证部门、工作组数据流安全，隔离广播域，提高网络性能。如果虚拟网之间的通信通过交换机的第 3 层功能进行网络分段管理，还可以提供第 3 层各网段间数据传输的安全控制。

3）安全策略的管理：

访问策略的合理使用能够在很大程度上防止不必要的网络连接，并且能够阻止非法的访问，提高网络的安全性。在防火墙上合理的规划使用访问策略及安全规则可以把阻挡网络外部的非法连接、病毒、攻击等，在接入层路由器或三层交换机上合理使用访问策略及安全规则能控制内部的非法访问，提高核心网络的安全性。

具体处理流程如下：

1）用户发起配置变更请求，说明需求及实现结果。

2）首信公司根据网络实际情况进行配置规划，并进行记录及制定回退方案。

3）用户审核确认后由首信公司服务工程师进行现场实施。

4）首信工程师与用户共同测试，验证需求是否完全实现，对最终配置进行本机备份，同时将配置文档上传配置库。

5）填写并提交《常规业务配置服务记录》，并由用户评估服务质量。

6）首信公司返回派工单，并由用户签字确认后双方存档。

7）定期备份用户网络配置，并上传用户存档。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 网络设置、网络管理、策略调整服务 | 根据用户业务需要对网络及安全设备进行配置变更，并做好备份及配置文档管理。 | 5 天×8 小时 |

**7. 日志审查**

及时查看网络设备和安全设备的系统日志，并定期分析系统相关日志信息。

**（1）服务内容**

首信公司运维人员在每次巡检及出现故障时，检查设备日志信息，并对日志信息进行统计、分析。通过查看交换机、路由器和其他安全设备的日志，可以迅速了解设备状态、运行状态和故障信息，从而快速发现和解决问题。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 日志审查服务 | 对用户网络及安全设备的日志进行统计和分析。 | 5 天×8 小时 |

**8. 网络流量分析服务**

提供全局网络流量监控分析服务，对网络流量基于应用层特征进行流量分析、统计，保障关键应用运行效率。分析应用响应延时、网络延时、服务器延时，分析网络利用率、网络效率、数据包重传，对 TCP 连接做健康分析并制定管理策略。

**（1）服务内容**

首信公司通过流量管理系统对全网的网络流量、负荷进行监测和排名统计。通过采集网络各个环节、所有设备、所有链路的流量负荷信息，并采用分级用户管理机制，随时为各种业务提供流量查询服务，及时为用户提供流量图及统计、分析结果，使用户能够清晰了解使用的带宽，并提供流量分析报告。

通过流量负荷定位，管理员可以快速诊断并发现负荷最高的链路，带宽占用最大的链

路，从而分析网络变慢、丢包的原因，能够按时形成数据流图形，可按 TopN 排序方式结合网络拓扑结构图进行定位，以显示网络流量分布情况，从业务、地域、用户多角度协助管理员分析用户网络流量行为，并在发生流量异常的时候进行预警，预防由于滥用网络带宽造成网络瘫痪。通过对 TCP、UDP 时行健康状态分析，根据数据包状态制定相应的管理策略，以保证各业务系统的稳定运行。主要通过以下方面进行监控：

1) 网络流量实时监控、超量警示、流量分析、告警历史记录回放、支持多种常用的智能分析功能，提供各种排名分析；
2) 全局流量统计：从整体角度对网络流量的数据包情况进行统计，包括数据包的长度、总体流量、总体协议分布、总体 TCP/IP 协议分布、TCP/UDP 端口分布等；
3) 终端流量统计：对终端流量进行统计和排序，并提供终端流量矩阵视图；
4) 从协议角度对网络数据行为进行分析，并按照终端形成排名，便于管理员掌握网络中协议的分布和重点终端的数据行为；
5) 提供对流量的流向进行分析，并对 TCP 会话进行监测，监测 TCP 会话分部，从而获取各个网络节点的流量和会话统计信息。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 网络流量分析服务 | 对用户网络流量进行统计和分析，对网络流量和数据包异常情况进行处理，根据分析结果制定相对应的管理策略。 | 5 天×8 小时 |

## 二、安全运维服务方案

### 1．安全设备定期巡检与监控

提供中心大楼安全设备巡检服务，根据中心大楼安全系统环境制订巡检方案，按计划对所有网络安全设备运行状况进行现场检查，收集设备运行参数，并提供《安全设备巡检报告》。

1) 安全监控是通过对操作系统的日志分析和网络实时监控等方式对系统行为、网络行为进行审计，及时检查安全隐患，发现安全事件。

2) 安全监控一般包括对系统的任何未经授权的访问以及操作系统本身是否存在安全

漏洞等两个方面，安全监控的对象主要包括用户帐号、网络行为和文件系统三个方面。

3） 管理员应每年对系统进行扫描，以及时发现系统漏洞。

4） 系统漏洞扫描前，管理员应提出扫描申请，描述扫描时间、扫描范围、及扫描可能造成影响及应急措施等。扫描申请获得批准后，方可进行扫描。

5） 扫描完毕后，应会同安全管理员分析扫描结果。

6） 针对扫描分析结果，应进行适当的处置，对高风险的漏洞及时出具修补措施。

7） 通过对用户帐号的登陆和用户行为进行审计，探测非授权访问和非法登陆尝试等。

8） 通过对主机的网络服务监控以及基于网络的入侵监测系统探测对系统的网络攻击行为。

9） 通过对文件系统安全的监控，保证文件系统的完整性，防止对于文件系统的非法访问，监控文件备份策略和规范是否得到了切实的执行。

### 2. 安全系统加固与优化

根据前期的安全巡检结果，根据北京市残疾人示范中心安全需求和业务流程制定安全加固优化方案，在不影响北京市示范中心业务开展的前提下，定期对操作系统、安全设备等的安全配置策略进行加强，及时消除因安全漏洞被恶意攻击者利用从而引发的风险。

政府行业用户普遍存在业务系统相对独立，网络系统所涉及的产品较多，因此，在信息系统网络拓扑结构方面相对复杂。由于政府电子政务系统建设，采取边建设边维护的模式。因此，每次系统结构的优化调整，都将会影响信息安全整体目标的调整。

首信公司将从信息安全的角度出发，逐步趋于合理，提出合理的优化加固方案，从整体结构上提高抗风险能力。

#### （1）系统脆弱性加固

通过技术手段，对正在运行的系统进行脆弱性扫描，包括网络设备、主机操作系统、关键应用系统等，发现系统当前各种漏洞，了解服务器系统整体安全状况。

操作系统安全策略配置的检查、运行日志的分析、系统补丁的升级查看、防病毒代码的更新审核等工作，最终完成北京市规划和国土资源管理委员会服务器操作系统的安全加固工作，具体工作内容包括：

- 安装最新补丁；
- 禁止不必要的应用和服务；

- 禁止不必要的账号；
- 去除后门；
- 内核参数及配置调整；
- 系统最小化处理；
- 加强口令管理；
- 启动日志审计功能；
- 利用定制脚本进行加固等。

**（2）安全设备配置策略优化加固**

通过前期对用户信息系统的风险评估以及定期巡检等工作，结合用户的实际需求，对安全配置策略提出有针对性的系统优化和加固方案。

- **安全设备部分安全加固项**

| 对象 | 安全子类 | 技术要求 |
| --- | --- | --- |
| 设备安全策略 | 结构安全 | 1. 根据网络不同功能区域、业务性质合理划分VLAN； |
| | 访问控制 | 2. 各业务 VLAN 间启用必要的安全访问控制措施；<br>3. 合理设置非活跃会话超时连接自动终止策略；<br>4. 宜采用 IP 和 MAC 绑定措施防止地址欺骗； |
| | 安全审计 | 5. 启用日志审计功能，对系统登录及各接口常见协议的启用和关闭等网络行为进行记录；<br>6. 确保设备的系统时间准确； |
| | 网络设备防护 | 7. 对通过 Telnet、Console 口和 AUX 口等各种登录设备的方式都进行认证；<br>8. 对管理员的登录 IP 地址进行限制；<br>9. 登录口令具有复杂度要求并定期更换，对短时间内错误登录次数进行限制；<br>10. 采用 SSH 工具对设备实施远程管理；<br>11. 关闭 Finger、FTP 和 HTTP 等不必要的危险服务；<br>12. 不使用的物理端口在配置上将其关闭； |
| | 入侵防范 | 13. 根据设备性能配置，启用对 IP 欺骗攻击、DDOS 攻击、端口扫描等网络攻击的防范功能； |
| | 恶意代码防范 | 14. 配置 ACL 对已知病毒所使用的 TCP、UDP 端口号进行过滤。 |

- **操作系统部分安全加固项**

Windows 操作系统：

| 分类 | 安全加固方法 |
| --- | --- |
| **账户和口令安全策略** | 设置合适的账号和口令策略 |
| | 设置口令设置的历史记录进行比对 |
| | 禁用或修改 administrator 账号 |
| | 禁用 guest 账号和其他无用账号 |
| | 对账号启用安全审计策略 |
| **磁盘分区及文件系统安全** | 磁盘分区的文件系统建议采用 NTFS 的格式 |
| | 关闭 IPC$远程默认共享 |
| | 关闭 C$、D$、E$等默认共享 |
| | 优化用户自主建立的远程共享，不允许匿名访问 |
| **调整系统开放的服务和端口** | 禁用不必要的 ftp 服务 |
| | 禁用不必要的 snmp 服务并且使用默认的 snmp 团体名 |
| | 禁用 Alerter、ComputerBrowse、DHCPClient 等服务 |
| **系统关键文件安全性** | 需要合理设置系统安装目录下 windows\system、windows\system32 等文件的安全属性 |
| **访问控制** | 调整系统的远程控制方式 |
| | 限制 LSA 匿名远程访问 |
| | 禁止 logon 对话框中出现 shutdown 按钮 |
| | 在屏幕登陆提示框中，不显示上次系统登陆的账号 |
| | 禁止系统缓冲区中保存的上次登陆账号 |
| **日志安全配置** | 系统日志安全配置 |
| | 安全日志安全配置 |
| | 应用程序日志安全配置 |
| **系统安全补** | 升级操作系统的安全补丁 |

| | |
|---|---|
| 丁 | 升级应用程序或安装应用程序安全补丁 |

国产操作系统：

| 分类 | 安全加固方法 |
|---|---|
| **账户及口令安全策略** | 启用加密口令文件/etc/shadow |
| | 加强账号及口令安全策略 |
| | 禁用不需要的账号 |
| | 删除用户建立的过期或无用的账号 |
| **系统文件安全属性** | 设置系统关键文件权限 |
| | 设置 root 账号的 umask |
| **系统访问安全** | 禁止 Ctrl+Alt+Delete 重新启动机器 |
| | 调整系统远程访问协议 |
| | 限制只有授权用户可以访问 at/cron |
| | 禁止 root 账号远程登陆 ftp 服务 |
| | 限制某些账号可以 su 到 root 账号 |
| | 配置主机防火墙 |
| | 限制 root 直接远程登陆 |
| | 禁止匿名登陆 ftp 服务器 |
| | 修改系统在登陆时暴露有关操作系统版本信息 |
| | 调整服务器的运行级别 |
| **系统开放的服务或端口** | 禁用不必要的 ftp 服务 |
| | 禁用不必要的 snmp 服务并且使用默认的 snmp 团体名 |
| | 禁用不必要的 syslog 服务 |
| | 禁用系统默认运行级别的/etc/rc*.d 目录中存在不用的服务 |
| | 关闭其它不需要的服务或端口 |

| | |
|---|---|
| **安装包和安全补丁** | 定期安装系统安全补丁 |
| | 卸载默认安装的不需要的安装包 |
| **系统日志安全配置** | 系统日志安全配置 |
| | 定期审计系统运行日志 |
| | 指定专用的 syslog 服务器记录日志 |
| **其它安全设置** | 打开 TCPSYN 的保护机制 |
| | 禁止接收、转发源路由数据包 |
| | 对系统的资源使用作限制 |
| **Linux 系统安全补丁** | 升级系统安全补丁 |
| | 升级应用程序的安全补丁 |

### 3. 终端入网审核服务

协助制定大楼网络接入技术标准及相关规范，提供大楼终端网络接入及符合性审核服务，确保接入大楼网络的计算机符合相关规定及标准，及时处理终端网络连接方面的问题。

提供大楼网络布线系统维修、维护，信息点调整及资料更新等服务；提供大楼网络的状态监控，故障诊断，快速恢复及现场运维等服务。

#### （1）服务内容

首信公司将根据用户相关标准进行终端入网的管理，禁止用户在未授权情况接入网络。对使用不良软件或进行不恰当的网络操作等行为，辅以有效的安全管理策略和规范，并对终端用户加以规范和引导。最终加强对桌面终端的有效安全防护，从而提升整体网络安全性。

定期对大楼机房进行清扫，整理配线架线路顺序，按规范连接跳线至交换机网点顺序，清理无用的跳线，对已损坏的网点配线架进行修复，同时打印粘贴网点标签，并将详细信息进行记录、归档。

对大楼网络的状态进行监控。在出现故障时，现场工程师将第一时间进行故障诊断，判断故障点后快速响应，将根据故障情况进行现场或远程处理，及时恢复网络中断或业务

中断故障。

**（2）服务标准**

| 服务类型 | 服务目标 | 服务响应 |
| --- | --- | --- |
| 终端入网审核服务 | 协助用户完成终端入网相关审核工作，并处理终端入网故障。掌握楼内网络接入终端网络使用情况，屏蔽不安全的设备和人员接入网络，规范用户接入网络的行为。针对市用户信息点使用进行管理。 | 5天×8小时 |

## 三、机房运维服务方案

首信公司负责中心机房的日常管理工作，包括机房内服务器、网络设备、安全设备定期巡检、故障排查、维护等。

负责机房机房基础环境的日常巡检及维护，机房人员进出、设备进出管理，以及故障排查和处置。

### 1. UPS系统

A. 每日巡检服务

- 配合维保单位进行故障备件更换
- 配合维保单位进行电池定期放电服务
- 模块5×8小时现场服务（不含法定节假日）
- 根据巡检内容出具相关巡检记录报告。

B. 故障处理服务

首信公司应根据故障的具体情况，及时联系维保单位采取必要的服务措施(包括调整)，尽快修复，恢复系统正常运行。服务时间7X24小时，响应时间30分钟，完成时间8小时。

C. 技术支持服务

首信公司根据采购人需求，通过电话或现场方式为采购人提供技术支持服务，协助采购人解决该系统日常运行中的问题。

### 2. 空调系统

A. 每日巡检服务

（1）机房空调制冷系统是否正常

（2）机房空调室外机运行是否正常

（3）机房温湿度是否正常

（4）根据巡检内容出具相关巡检记录报告。

B. 故障处理服务

首信公司应根据故障的具体情况，及时联系维保单位采取必要的服务措施(包括调整)，尽快修复，恢复系统正常运行。服务时间 7X24 小时，响应时间 30 分钟，完成时间 4 小时。

C. 技术支持服务

首信公司根据采购人需求，通过电话或现场方式为采购人提供技术支持服务，协助采购人解决该系统日常运行中的问题。

## 四、会议保障服务方案

首信公司负责中心会议系统、音响系统及显示系统的调试及会议保障工作，保障会议室音、视频正常使用，视频会议通信线路通畅，提供会议全程保障，并根据会议需求适时调节音量，遇到问题及时处理。

## 五、其他运维服务方案

### 1．现场技术支持

#### （1）服务描述

首信公司提供一名经验丰富的技术支持工程师，进行全年 5×8 小时的现场支持服务，已保障网络运行中出现问题及时处理，并参与采购人分配的其它临时性维护任务。

#### （2）服务应答

首信公司现场工程师将负责以下服务工作：

1) 负责各种计算机外部设备的维护:包括打印机、扫描仪、投影机等；

2) 负责各会议室的非涉密会议设备调试及会议保障工作；

3) 负责电话系统维护：包括各办公室分机电话的安装调试；

4) 在必须进行网络系统重装或重启等较大操作时，须经采购人批准方可实施。

5）首信公司服务人员在处理故障后，要向采购人维护人员解释故障原因和解决方法，以及在日常维护中的预防措施。

6）首信公司服务人员在处理故障完毕后，要认真撰写《故障处理报告》，并提交采购人。

**2．电话技术支持**

**（1）服务描述**

首信公司通过电话为采购人提供技术支持服务，协助采购人解决网络系统日常运行中的问题。

**（2）服务应答**

1）首信公司应设立7×24小时的技术支持热线，保证采购人获得网络系统日常维护的技术支持，保证采购人关于网络系统的技术性问题得到及时、有效的解答。

2）首信公司保证技术支持热线电话95%以上的呼叫接通时间小于30秒；当首信公司需要查阅相关资料再对采购人的问题进行回复时，应确保在30分钟内回复。

**3．机房基础环境服务**

首信公司提供机房基础环境设备的技术支持和运行维护服务，定期巡检，及时排除故障，确保系统稳定、正常、连续的工作。

**（1）UPS系统**

D. 每日巡检服务

- 配合维保单位进行故障备件更换
- 配合维保单位进行电池定期放电服务
- 模块5×8小时现场服务（不含法定节假日）
- 根据巡检内容出具相关巡检记录报告。

E. 故障处理服务

首信公司应根据故障的具体情况，及时联系维保单位采取必要的服务措施(包括调

整)，尽快修复，恢复系统正常运行。服务时间 7X24 小时，响应时间 30 分钟，完成时间 8 小时。

F. 技术支持服务

首信公司根据采购人需求，通过电话或现场方式为采购人提供技术支持服务，协助采购人解决该系统日常运行中的问题。

**（2）空调系统**

D. 每日巡检服务

（1）机房空调制冷系统是否正常

（2）机房空调室外机运行是否正常

（3）机房温湿度是否正常

（4）根据巡检内容出具相关巡检记录报告。

E. 故障处理服务

首信公司应根据故障的具体情况，及时联系维保单位采取必要的服务措施(包括调整)，尽快修复，恢复系统正常运行。服务时间 7X24 小时，响应时间 30 分钟，完成时间 4 小时。

F. 技术支持服务

首信公司根据采购人需求，通过电话或现场方式为采购人提供技术支持服务，协助采购人解决该系统日常运行中的问题。

**4. 定期巡检服务**

**（1）服务描述**

首信公司为采购人的网络系统进行定期的现场检查，及时发现网络系统运行中出现的隐患，通过设备巡检手段，减少系统发生故障的概率，保证系统稳定、高效运行。

**（2）服务应答**

1) 首信公司每月进行一次现场设备运行情况检查，对采购人网络及安全设备进行细致全面监视和检查，对系统做预防性维护，减少潜在故障发生。

2） 首信公司在巡检完成后 3 个工作日内提交《巡检报告》。

**5. 故障处理服务**

**（1）服务描述**

首信公司应根据故障的具体情况，采取必要的服务措施(包括调整)，尽快修复，恢复网络系统正常运行。首信公司可通过电话指导、现场服务等方式进行故障诊断与处理，并保证满足双方约定的服务等级中的处理时限。

**（2）服务应答**

1） 首信公司根据采购人网络平台情况，利用网络管理与远程监控工具、手段，进行日常网络的流量、链路状态、设备运行情况等监控管理，并提安全预警服务。

2） 要求网络系统可用性不小于 99%;

3） 首信公司提供 7×24 小时服务。电话支持服务、定期巡检服务。

4） 服务响应时间：

| 等级 | 第一次电话回复；故障确认 | 提出初步行动计划 | 服务时间 |
|---|---|---|---|
| 紧急 | 2 小时 | 8 小时 | 标准服务时间 |
| 重要 | 4 小时 | 24 小时 | 7×24 小时 |

**6. 常规网络配置服务**

**（1）服务描述**

在采购人提出需求的情况下，首信公司根据需求对网络设备进行配置，实现要求的功能。如对网络设备的 IP、VLAN、路由、ACL 等进行变更配置。

**（2）服务应答**

1） 按采购人提出的需求设计配置方案，并实施要求的功能。

2） 对变更的配置文件进行备份，并填写《配置变更记录》。

**7. 咨询服务**

**（1）服务描述**

1） 按需提供网络、业务规划、设计建议。

2） 针对采购方提出的信息化技术问题进行解答。

**（2）服务应答**

1） 首信公司将通过有效的运维管理方法，对客户进行日常网络运行服务，总结、分析网络运行过程中出现的问题，提出解决建议。

2） 首信公司现场服务中将工作整理成《技术文档》、详细记录各项工作的流程和内容，将故障发生的原因、处理过程、以及类似故障的预防和处理经验汇总成《知识库》，以便采购方随时查阅，驻场工程师将为采购方做详细解答、指导。项目经理定期参加采购人组织的运维例会。

**8. 文档服务**

**（1）服务描述**

制定完善的运维方案、应急情况处理方案，说明每日运维工作、每月运行报告等内容。其他文档还应包括：问题故障分析处理报告、技术手册、版本和补丁升级记录、巡检记录等内容。对运维过程中形成的过程和技术文档进行管理。

**（2）服务应答**

1） 首信公司定期或按需向采购人提供所需技术文档。

2） 首信公司保存并定期向采购人提交《服务确认单》，包括电子版和纸质签字版。

3） 首信公司每月向采购人提交《运维服务报告》。