磋商响应文件

采购项目名称: 西宁市人大代表网络履职平台软件运维项目

供应商： 六合远教（成都）科技有限公司 （公章）

法定代表人或委托代理人：___（签字或盖章）

年 月 日

1　磋商函

磋商函

致：西宁市人民代表大会常务委员会办公室

我们收到西宁市人民代表大会常务委员会办公室磋商文件，经研究，法定代表人（姓名、职务）正式授权（委托代理人姓名、职务）代表供应商（供应商名称、地址）提交磋商响应文件。

据此函，签字代表宣布同意如下：

1、我方已详阅磋商文件的全部内容，包括澄清、修改条款等有关附件，承诺对其完全理解并接受。

2、磋商有效期自磋商之日起 60 天内有效。如果在规定的磋商时间后，我方在磋商有效期内撤回磋商文件或成交后不签约的，承担相应法律责任。

3、我方同意按照贵方要求提供与磋商有关的一切数据或资料，理解并接受贵方制定的评标办法。

4、与本磋商有关的一切正式往来通讯请寄：

地址：_____　　邮编：_____

电话：_____　　传真：_____

法定代表人姓名：_____ 职务：_____

磋商响应单位：六合远教（成都）科技有限公司 （公章）

法定代表人或委托代理人： （签字或盖章）

年 月 日

2 法定代表人证明书

法定代表人证明书

致：西宁市人民代表大会常务委员会办公室

（法定代表人姓名）现任我单位_____职务，为法定代表人，特此证明。

法定代表人基本情况：

性别：___年龄：___民族：

地址：

身份证号码：

附法定代表人第二代身份证双面扫描（或复印）件

磋商响应单位： 六合远教（成都）科技有限公司 **（公章）**

年 月 日

3 法定代表人授权书

法定代表人授权书

致：西宁市人民代表大会常务委员会办公室

（供应商名称）系中华人民共和国合法企业，法定地址_____。

（法定代表人姓名）特授权（委托代理人姓名）_____代表我单位全权办理_____针对_____项目的磋商、答疑等具体工作，并签署全部有关

的文件、资料。

我单位对被授权人的签名负全部责任。

被授权人签署的所有文件（在授权书有效期内签署的）不因授权的撤销而失效。

授权期限：自磋商之日起 60 天。

被授权人联系电话：

授权人（法定代表人）签字或盖章：_____

职务：

被授权人（委托代理人）签字或盖章：_____

职务：

附被授权人第二代身份证双面扫描（或复印）件

磋商响应单位： 六合远教（成都）科技有限公司 （公章）

年 月 日

4 供应商承诺函

供应商承诺函

致：西宁市人民代表大会常务委员会办公室

关于贵方__年_月_日_____(项目名称)采购项目，本签字人愿意参加磋商，提供采购一览表中要求的所有服务，并证实提交的所有资料是准确的和真实的。同时，我代表（供应商名称），在此作如下承诺：

1、完全理解和接受磋商文件的一切规定和要求；

2、若成交，我方将按照磋商文件的具体规定与采购人签订采购合同，并且严格履行合同义务，按时提供优质的服务。如果在合同执行过程中，发现质量、数量出现问题，我方一定尽快处理，如果对甲方造成经济损失的，承担相应的经济责任。

3、我方保证甲方在使用该产品或其任何一部分时，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知识产权的起诉，若有违犯，愿承担相应的一切责任。

4、我方承诺，除磋商文件中规定的进口产品外，所投的产品均为国产产品，且均符合国家强制性标准。若有不实，愿承担相应的责任。

5、在整个磋商过程中我方若有违规行为，贵方可按磋商文件之规定给予处罚，我方完全接受。

6、若成交，本承诺将成为合同不可分割的一部分，与合同具有同等的法律效力。

磋商响应单位： 六合远教（成都）科技有限公司 **（公章）**

法定代表人或委托代理人： ___ **（签字或盖章）**

年 月 日

5 供应商诚信承诺书

供应商诚信承诺书

致：西宁市人民代表大会常务委员会办公室

为了诚实、客观、有序地参与采购活动，愿就以下内容作出承诺：

一、自觉遵守各项法律、法规、规章、制度以及社会公德，维护廉洁环境，与同场竞争的供应商平等参加采购活动。

二、参加本次采购活动时，严格按照磋商文件的规定和要求提供所需的相关材料，并对所提供的各类资料的真实性负责，不虚假应标，不虚列业绩。

三、尊重参与采购活动各相关方的合法行为，接受采购活动依法形成的意见、结果。

四、依法参加采购活动，不围标、串标，维护市场秩序，不提供“三无”产品、以次充好。

五、积极推动采购活动健康开展，对采购活动有疑问、异议时，按法律规定的程序实名（加盖单位章和法定代表人签名）反映情况，不恶意中伤、无事生非，以和谐、平等的心态参加政府采购活动。

六、认真履行成交供应商应承担的责任和义务，全面执行采购合同规定的各项内容，保质保量地按时提供采购物品。

若本企业（单位）发生有悖于上述承诺的行为，愿意接受相关处理。

本承诺是采购项目磋商文件的组成部分。

磋商响应单位：六合远教（成都）科技有限公司 （公

章）

法定代表人或委托代理人：___（签字或盖章）

年 月 日

6 供应商资格证明文件

供应商资格证明文件

资格证明材料包括：提供有效的营业执照、税务登记证、机构代码证或三证（五证）合一统一社会代码证及其他资格证明文件（扫描或复印件）。

1、企业法人需提交“统一社会信用代码的营业执照”，未换证的提交“营业执照、组织机构代码证、税务登记证”；

事业法人需提交“统一社会信用代码的事业单位法人证书”，未换证的提交“事业单位法人证书或组织机构代码证”；

其他组织需提交“统一社会信用代码的社会团体法人登记证书”或“统一社会信用代码的民办非企业单位登记证书”或“统一社会信用代码的基金会法人登记证书”，未换证的提交 “社会团体法人登记证书”或“民办非企业单位登记证书”或“基金会法人登记证书”和“组织机构代码证”；

个体工商户需提交“统一社会信用代码的营业执照”或“营业执照、税务登记证”；自然人需提交身份证明。

2、根据采购项目内容，提供供应商的相关资质证书、许可证等。

7 无重大违法记录声明

无重大违法记录声明

提供参加采购活动前 3 年内在经营活动中没有重大违法记录的书面声明，并附“信用中国”网站无任何不良记录的查询截图，时间为磋商截止时间前 10 天内。（格式可自定）

8　财务状况、缴纳税收和社会保障资金证明

财务状况、缴纳税收和社会保障资金证明

按照《政府采购法》第 22 条规定提供以下相关材料：

1、①供应商是法人公司的，提供 2025 年度经审计的财务状况报告，包括资产负债表、利润表、现金流量表及其附注包括审计方的营业执照、执业证书及审计人员的执业证书复印件；② 2025 年度新成立的企业附基本开户银行出具近 3 个月内的资信证明（同时提供基本存款账户开户许可证）；③供应商是其他组织和自然人，没有经审计的财务报告，可以提供基本开户银行出具近 3 个月内的资信证明（同时提供基本存款账户开户许可证）。

2、提供近半年内任意 1 个月企业依法缴纳税收和职工社会保障资金记录的证明材料。依法免税或不需要缴纳社会保障资金的供应商，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。

9　磋商最初报价表

磋商最初报价表

供应商名称（盖章）：　　日期：　年　月　日

项目名称	磋商总价（人民币：元）	服务期	备注
	大写：		
	小写：		
其他：			

注：1.填写此表时不得改变表格形式。

2.磋商报价为总报价。必须包括：包括项目编制费、服务费、税金及其他不可预见费等全部费用。

3.“服务期”是指完成服务所需的具体时间。

磋商响应单位：六合远教（成都）科技有限公司 （公章）

法定代表人或委托代理人：　　（签字或盖章）

年 月 日

10 服务要求响应表

服务要求响应表

供应商名称：六合远教（成都）科技有限公司

采购需求服务指标			磋商响应服务指标		偏离
序号	名称	服务要求、指标	名称	服务要求、指标	
1	**网络优化检测服务**	1.保障平台平稳安全运行，随时监控硬件以及软件使用情况。 2.采用软件自动	**网络优化检测服务**	我司承诺完全响应本项目的服务要求及指标： 1.保障平台平稳安全运	0

		化实时对硬件进行检测服务，合理分析硬件使用情况后在做出最优规划。 3.软件优化检测服务，通过人工配合优化监测软件完成，通过对软件参数设置取得的使用效果，测试软件承受范围内达到最高性能负载。根据测		行，随时监控硬件以及软件使用情况。 2.采用软件自动化实时对硬件进行检测服务，合理分析硬件使用情况后在做出最优规划。 3.软件优化检测服务，通过人工配合优化监测软件完	

		试数据，调整、优化软件建设规划。 4.结合硬件与软件检测报告，统计分析数据，逐步优化完善人大代表网络履职平台。		成，通过对软件参数设置取得的使用效果，测试软件承受范围内达到最高性能负载。根据测试数据，调整、优化软件建设规划。 4.结合硬件与软件检测报告，统计分析数据，逐步优	

				化完善人大代表网络履职平台。	
2	**平台计算资源维护**	1.保证平台硬件设备长期、正常运转，需要对服务器和相关设备的统计和标记工作；定时检查和保障服务器的维护工作，包括系统安装，系统补丁更新；对网络故障进行判断和	**平台计算资源维护**	我司承诺完全响应本项目的服务要求及指标：1.保证平台硬件设备长期、正常运转，需要对服务器和相关设备的统计和标记工作；定时检查和保障服	0

		排查。对服务器 2.使用安全措施 处理包括但不限 于 DDOS 攻击在 内的系统安全问 题。 3.需要定期测试 系统安全性，根 据现有系统架构 规划、调整安全 防护措施。 4.实时的对网络 流量进行监控， 处理异常问题。		务器的维护工 作，包括系统 安装，系统补 丁更新；对网 络故障进行判 断和排查。对 服务器 2.使用安全措 施处理包括但 不限于 DDOS 攻击在内的系 统安全问题。 3.需要定期测 试系统安全	

				性，根据现有系统架构规划、调整安全防护措施。 4.实时的对网络流量进行监控，处理异常问题。	
3	**平台软件维护**	1.根据《中华人民共和国网络安全法》要求，服务器主机、应用平台软件应满足《信息安全技术	**平台软件维护**	我司承诺完全响应本项目的服务要求及指标： 1. 根据《中华人民共和国网络安全	0

		网络安全等级保护基本要求》第三级安全要求（以下简称“等保三级”），对不满足等保三级标准的，及时发现，及时整改。 2.乙方应配合甲方进行等保三级测评工作。包括但不限于甲方需建立安全管理制度、方案编写等		法》要求，服务器主机、应用平台软件应满足《信息安全技术网络安全等级保护基本要求》第三级安全要求（以下简称“等保三级”），对不满足等保三级标准的，及时发现，及时整	

		工作的情况；对测评过程中需要乙方提供包括但不限于文字资料、技术支持的情况。 3.在使用过程中需要对系统程序本身、中间件、数据库、数据等进行维护保证平台正常运行。对程序本身、操作系统、中间件、		改。 2.乙方应配合甲方进行等保三级测评工作。包括但不限于甲方需建立安全管理制度、方案编写等工作的情况；对测评过程中需要乙方提供包括但不限于文字资料、技术支持	

		数据库出现漏洞的，需及时修复。漏洞来源包括但不限于国家、省、市网信或公安部门发布、平台涉及软件所属厂家发布、国内外知名安全厂家发布、乙方上级部门通知，甲方通知。 4.定时完成对系统程序、数据库		的情况。 3.在使用过程中需要对系统程序本身、中间件、数据库、数据等进行维护保证平台正常运行。对程序本身、操作系统、中间件、数据库出现漏洞的，需及时修复。漏洞来源包括	

		进行备份、恢复、临时数据统计分析。 5.根据网站优化检测结果对网站进行持续优化, 提出优化方案。 6.对西宁人大平台进行持续的优化和维护升级。 7.平台内无效或者问题链接定期处理，并对平台的网络安全进行		但不限于国家、省、市网信或公安部门发布、平台涉及软件所属厂家发布、国内外知名安全厂家发布、乙方上级部门通知，甲方通知。 4.定时完成对系统程序、数据库进行备	

		防护做出相关措施。		份、恢复、临时数据统计分析。 5.根据网站优化检测结果对网站进行持续优化，提出优化方案。 6.对西宁人大平台进行持续的优化和维护升级。 7.平台内无效或者问题链接	

				定期处理，并对平台的网络安全进行防护做出相关措施。	
4	**页面分布及内容修改**	1.采用技术措施全年完成至少一次全站内容安全检测，每篇信息发布前采用技术措施进行内容安全检测，确保信息发布准确无误。	**页面分布及内容修改**	我司承诺完全响应本项目的服务要求及指标：1.采用技术措施全年完成至少一次全站内容安全检测，每篇信息发布前采用技	0

		2.根据甲方的要求对页面分布、数据、内容进行适当调整。 3.根据甲方的需要，建设1-2个专题栏目。		术措施进行内容安全检测，确保信息发布准确无误。 2.根据甲方的要求对页面分布、数据、内容进行适当调整。 3.根据甲方的需要，建设1-2个专题栏目。	
5	**微信公众**	根据甲方需求，	**微信公**	我司承诺完全	0

	号及门户网站信息发布	负责“西宁人大”微信公众号的日常内容更新与维护、负责西宁人大门户网站的内容更新与维护，发布前进行人工复审。	**众号及门户网站信息发布**	响应本项目的服务要求及指标：根据甲方需求，负责“西宁人大”微信公众号的日常内容更新与维护、负责西宁人大门户网站的内容更新与维护，发布前进行人工复审。	
6	**培训**	供应商需对甲方	**培训**	我司承诺完全	0

		业务操作人员、技术维护人员运维服务期内进行不少于一次业务、技术及安全培训。		响应本项目的服务要求及指标：供应商需对甲方业务操作人员、技术维护人员运维服务期内进行不少于一次业务、技术及安全培训。	

注：1.本表应按照第五部分“（二）运维项目采购需求”中序号的指标逐项填写，不得遗漏。

2.填写此表时以招标项目参数要求为基本磋商响应要求，满足招标项目参数要求的指标需列出“0”；超出、不满足招标项目参数要求的指标需列出“+”、“-”偏差，并做出详细说明。

3.供应商响应采购需求应具体、明确，含糊不清、不确切或伪造、编造证

明 材料的，按照实质性不响应处理。对伪造、编造证明材料的，将报告本级财政部门。

磋商响应单位：六合远教（成都）科技有限公司 （公章）

法定代表人或委托代理人： （签字或盖章 ）

年 月 日

11 供应商的类似业绩证明材料

供应商的类似业绩证明材料

提供自 2025 年以来的类似业绩证明材料。类似业绩是指与采购项目在服务类型、使用功能、合同规模等方面相同或相近的项目。需提供包含合同首页、标的及金额所在页、供货合同签字盖章页的扫描件（或复印）件。

12 供应商认为在其他方面有必要说明的事项

12.1 团队人员

西宁市人大代表网络履职平台团队人员配置情况如下：

项目小组岗位	名单	政治面貌	职称
项目负责人	石研	党员	高级信息系统项目管理师
项目运维经理	王飞	党员	中级系统集成项目管理工程师 网络通信安全管理员
技术经理	陈虎	党员	麒麟操作系统运维高级工程师

研发工程师	代红云	预备党员	麒麟操作系统运维高级工程师
研发工程师	汪义强		麒麟操作系统运维高级工程师
研发工程师	钟铖		麒麟操作系统运维高级工程师
项目经理	唐厚湖	/	/
运营编辑	赵元存	入党积极分子	/
运营编辑	朱自越	群众	/
客服人员	郭培鹏	入党积极分子	/
研发工程师	梁明川	/	/
UI 设计	曾彬	/	产品专家称号

12.1.1 项目负责人

石研身份证

石研高级信息系统项目管理师证书

石研在职证明

12.1.2 项目运维经理

王飞身份证

王飞中级系统集成项目管理工程师证书

王飞网络通信安全管理员证书

王飞在职证明

12.1.3 核心技术团队人员

12.1.3.1 核心技术团队成员陈虎

陈虎身份证

陈虎麒麟操作系统运维高级工程

陈虎在职证明

12.1.3.2 核心技术团队成员代红云

代红云身份证

代红云麒麟操作系统运维高级工程

代红云在职证明

12.1.3.3 核心技术团队成员汪义强

汪义强身份证

汪义强麒麟操作系统运维高级工程

汪义强在职证明

12.1.3.4 核心技术团队成员钟铖

钟铖身份证

钟铖麒麟操作系统运维高级工程

钟铖在职证明

12.2 总体运维服务方案

12.2.1 服务概述

本方案旨在确保西宁市人大代表网络履职平台的平稳、安全、高效运行。通过网络优化检测、平台计算资源维护、平台软件维护、页面分布及内容修改、微信公众号及门户网站信息发布、以及培训等服务，全面提升平台的性能和安全性。

12.2.2 服务需求分析

网络优化检测服务：保障平台平稳安全运行，实时监控硬件和软件使用情况，优化硬件和软件性能。

平台计算资源维护：保证平台硬件设备长期正常运转，处理系统安全问题，定期测试系统安全性，实时监控网络流量。

平台软件维护：满足《信息安全技术网络安全等级保护基本要求》第三级安全要求，维护系统程序、中间件、数据库等，及时修复漏洞。

页面分布及内容修改：确保信息发布准确无误，调整页面分布和内容，建设专题栏目。

微信公众号及门户网站信息发布：负责“西宁人大”微信公众号的日常内容更新与维护，负责西宁人大门户网站的内容更新与维护，发布前进行人工复审，确保信息发布准确无误。

培训：运维服务期内对业务操作人员和技术维护人员进行不少于一次业务、技术及安全培训。

12.2.3 各项服务的具体措施

12.2.3.1 网络优化检测服务：

实时监控硬件和软件使用情况。

采用自动化软件进行硬件检测，合理分析硬件使用情况。

通过人工配合优化监测软件，调整软件参数，优化软件建设规划。

结合硬件与软件检测报告，统计分析数据，逐步优化平台。

12.2.3.2 平台计算资源维护：

定时检查和维护服务器，包括系统安装和补丁更新。

处理网络故障，使用安全措施应对 DDOS 攻击等系统安全问题。

定期测试系统安全性，调整安全防护措施。

实时监控网络流量，处理异常问题。

12.2.3.3 平台软件维护：

满足等保三级安全要求，及时发现并整改不符合标准的部分。

配合甲方进行等保三级测评工作，提供必要的文字资料和技术支持。

维护系统程序、中间件、数据库等，及时修复漏洞。

定时备份和恢复系统程序和数据库，进行临时数据统计分析。

根据网站优化检测结果，提出优化方案。

对西宁人大平台进行持续的优化和维护升级。

平台内无效或者问题链接定期处理，并对平台的网络安全进行防护。

12.2.3.4 页面分布及内容修改：

根据甲方的要求，结合人大代表网络履职平台的实际使用需求，我司从页面布局、栏目结构、内容安全、适老化与无障碍、移动端适配、检索体验等方面对西宁人大网及平台页面进行持续调整与优化，具体措施如下：

（1）. 页面布局与栏目结构优化

结合人大代表履职场景与群众浏览习惯，对首页及代表履职、监督工作、议案建议、学习培训等栏目的版块顺序、层级与留白逐项梳理，将代表和群众最常用的履职服务入口前置，压缩冗余层级，使信息层级清晰、访问路径更短。

（2）. 专题栏目与重大会议活动页面建设

按甲方需要，每个运维服务期建设 1-2 个专题栏目。围绕人民代表大会会议、代表专题调研、代表主题活动、规范性文件宣传等重点工作，提供专题页面策划、版式设计、数据组织与上线维护，做到主题突出、更新及时、归档规范。

（3）. 内容安全检测与发布前审核

采用技术措施建立全站内容安全检测机制，对全站稿件、外链、图片及附

件进行扫描排查；每篇信息发布前先经技术措施检测、再由编辑与负责人逐级人工复审，重点核查政治性表述、涉密信息与文字差错，做到发布内容零差错。

（4）． 适老化与无障碍改造

网站与平台面向人大代表及社会公众，按无障碍规范提供字号放大、对比度提升、语义化标签与图片替代文本，保证老年用户与残障用户能够顺利浏览、查询所需信息。

（5）． 移动端适配与访问体验

针对手机端访问比例较高的特点，采用响应式布局对页面进行适配，保证页面在不同屏幕与分辨率下显示完整、字号可读、按钮可点，并与代表履职移动端应用保持一致的视觉与交互体验。

（6）． 检索与访问性能优化

对站内检索、栏目导航与常用服务入口进行可用性优化，通过图片压缩、资源合并、页面缓存与静态化等手段提升页面打开速度，保障业务高峰及重要会议期间的访问稳定性。

上述措施在运维服务期内按季度组织实施，形成页面优化记录与内容安全

检测报告，提交甲方确认，实现页面与内容的持续优化。

每年进行至少一次全站内容安全检测，每篇信息发布前进行内容安全检测。

根据甲方要求调整页面分布、数据和内容。

建设 1-2 个专题栏目。

12.2.3.5 微信公众号及门户网站信息发布：

负责“西宁人大”微信公众号的日常内容更新与维护，围绕代表履职动态、监督工作、代表风采、公告通知等栏目开展选题策划、图文编辑、排版校验与发布，保障公众号更新频次与内容质量。

负责西宁人大门户网站的内容更新与维护，及时发布人大常委会会议、监督工作、代表活动、人事任免、决议决定等信息，保障各栏目内容及时准确、版式统一。

信息发布前实行“编辑初审＋负责人复审”的双人审核机制，重点核查政治性表述、领导姓名职务、数据引用与图片说明，确保发布内容准确无误。

建立内容发布台账，逐篇登记发布日期、所属栏目、审核人与发布人，做到

发布留痕、责任可溯，并定期向甲方报送发布统计。

定期巡检微信公众号与门户网站发布渠道及账号权限，落实账号口令定期更换、操作终端安全检查等措施，防范账号被盗用、内容被篡改。

12.2.3.6 培训：

为了确保业务操作人员和技术维护人员能够全面理解和掌握各项业务流程、技术要点以及安全保障措施，公司规定必须定期对他们进行不少于一次的业务、技术及安全培训。通过这种培训，旨在提高操作人员的专业技能，增强业务处理效率，同时确保在工作中能够严格遵守操作规程和安全规范，以防潜在的风险和意外事故的发生。

在业务培训方面，将涵盖业务流程的各个环节，操作人员都需要熟悉并掌握每一个细节。技术维护培训则侧重于最新的技术动态和系统维护知识，以确保技术人员能够熟练运用先进技术解决实际问题。同时，安全培训也是不可或缺的部分，它将为操作人员提供识别风险、防范安全威胁的基本技能，并在发生安全事件时能够迅速响应和处理。

12.2.4 运维服务质量保证措施

定期检查和维护是确保硬件和软件正常运行的重要措施。通过对它们进行定期的检查和维护，可以及时发现并解决潜在的问题，从而保证平台的稳定性和可靠性。此外，定期检查和维护还可以提高硬件和软件的性能，延长它们的使用寿命。实时监控是对硬件和软件使用情况的持续跟踪和监测。通过实时监控，可以及时发现硬件和软件的异常情况，并采取相应的措施进行处理，以避免问题的扩大和影响。安全防护是保障平台安全的重要环节。采用多种安全措施，如防火墙、入侵检测系统、数据加密等，可以有效防止外部攻击和内部泄露，确保平台的数据和信息的安全。优化调整是根据检测结果和用户反馈，对平台进行持续的改进和调整。通过优化调整，可以提高平台的性能，满足用户的需求，提升用户体验。当然，继续扩展这个主题，我们可以深入探讨每一个环节的细节以及它们如何共同构建一个高效、稳定且安全的平台环境。

定期检查和维护：这一过程不仅限于简单的“检查并修复”。它包括了深度分析硬件健康状况，如硬盘的 SMART 数据、内存的错误检查、以及 CPU 和

GPU 的负载情况。软件方面，则涉及更新补丁、优化配置、以及清理不必要的文件和日志，确保系统干净、高效。此外，对于关键系统，还应进行定期的备份和恢复演练，以应对可能的灾难性事件。

实时监控：实时监控不仅仅是监视硬件和软件是否在运行。它还需要能够实时分析性能数据，如响应时间、吞吐量、资源利用率等，以便在问题出现之前进行预测和调整。同时，对于安全监控，还需要能够实时检测异常行为和网络流量，防止潜在的安全威胁。为了实现这一目标，平台应部署先进的监控工具，这些工具能够自动收集、分析和报告关键性能指标和安全事件。

安全防护：除了上述提到的安全措施外，还应考虑实施多层次的防御策略。这包括使用强密码策略、实施访问控制和权限管理、定期进行安全审计和漏洞扫描等。

优化调整：优化调整是一个持续的过程，它需要根据平台的使用情况和用户需求进行动态调整。这可能包括调整硬件配置以提高性能、优化软件代码以提高效率、改进用户界面以提高用户体验等。为了实现这一目标，平台应建立一

个完善的反馈机制，收集用户反馈和意见，并定期进行性能评估和用户满意度调查。

12.2.5 考核标准

平台稳定性：平台运行稳定，无重大故障。

安全性：平台符合等保三级安全要求，无重大安全漏洞。

优化效果：平台性能持续优化，用户体验良好。

培训效果：业务操作人员和技术维护人员掌握必要的技能，能够独立处理常见问题。

内容发布：微信公众号及门户网站信息发布前经人工复审，全年无内容发布差错、无内容安全事件。

响应时效：5×8 小时日常技术支持、7×24 小时应急支持，一般问题 30 分钟内响应、2 小时内解决，紧急事件按应急预案处置。

结合上述考核标准根据客户要求指定考核表，对整体运维服务工作进行评定。

12.3 应急响应服务方案

12.3.1 总则

为加强和规范西宁市人大常委会办公室信息系统网络安全工作，提高网络安全防护水平，实现网络安全的可控、能控、在控，依据国家有关法律、法规的要求，制定本文档。

12.3.1.1 目标

以满足业务运行要求，遵守行业规程，实施等级保护及风险管理，确保网络安全以及实现持续改进的目的等内容作为本单位网络安全工作的总体方针。以信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断为总体目标。

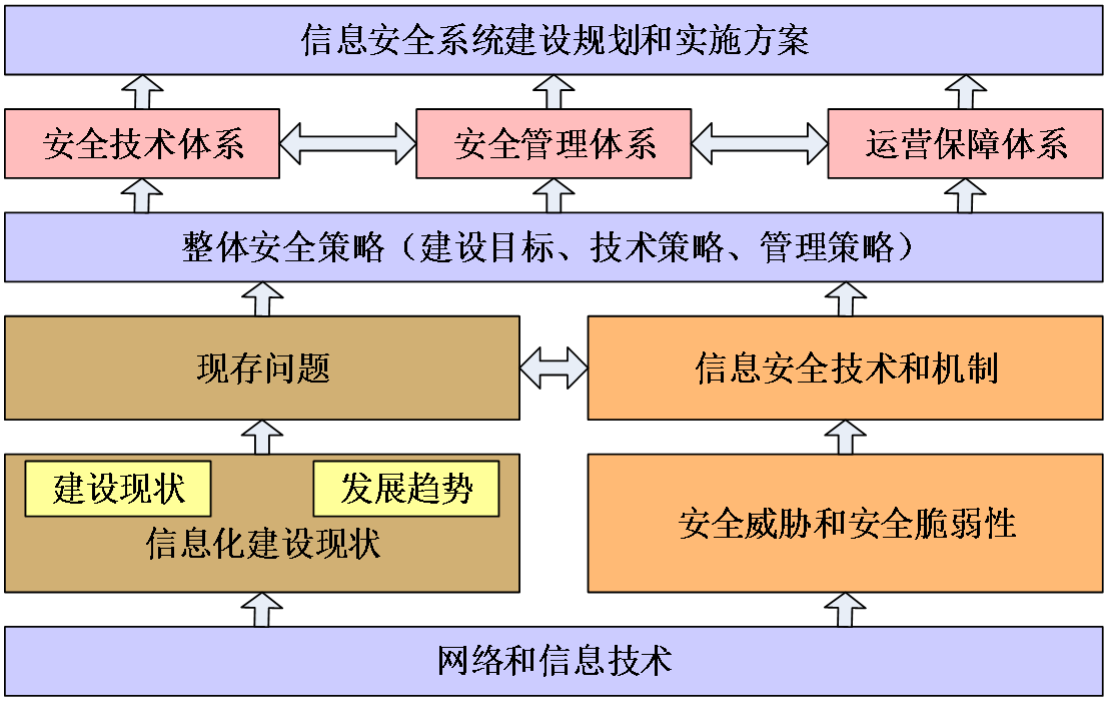
12.3.1.2 适用范围

本文档适用于网络安全方案规划、安全建设实施和安全策略的制定。在全

单位范围内给予执行，由网络和信息化安全领导小组对该项工作的落实和执行进行监督，由技术部配合网络和信息化安全领导小组对本案的有效性进行持续改进。

12.3.1.3 建设思路

西宁市人大常委会办公室信息系统网络安全建设工作的总体思路如下图所示：



信息化建设是基于当前通用的网络与信息系统基础技术，针对安全性问题

和支撑安全技术，通过安全评估，对信息化建设和网络安全建设进行分析和总结，其中包括对建设现状和发展趋势的完整分析，归纳出系统中当前存在和今后可能存在的安全问题，明确网络和信息系统运营所面临的安全风险级别。

从支撑性安全技术展开，对现有网络和信息技术的固有缺陷出发，总结了普遍存在的安全威胁，并根据其它系统中的网络安全建设实践中的经验，从网络安全领域的完整框架、思路、技术和理念出发，提供完整的安全建设思路和方法。

在此基础之上，对网络安全领域的理论、框架和技术基础与西宁市人大常委会办公室信息系统的安全问题有机地进行结合，有针对性地提出西宁市人大常委会办公室信息系统安全保障总体策略。安全保障总体策略包括了整体建设目标，安全技术策略，以及相应的管理策略。

以安全保障总体策略为核心，分三个方面进行整体网络安全体系框架的制定，包括安全技术体系，安全管理体系和运营保障体系。在现实的运营过程中，安全保障不能够纯粹依靠安全技术来解决，更需要适当的安全管理，相互结合

来提高整体安全性效果。

在网络安全体系框架的指导下，依据相应的建设标准和管理规范，规划和制定详细的网络安全系统实施方案和运营维护计划。

网络安全体系建设的思路体现了以下的特点：

- 统筹规划和设计在建设过程中占有非常重要的地位；
- 充分结合建设现状与网络安全通用技术和理念；
- 充分考虑了当前的建设现状以及未来业务发展的需要；
- 注重安全管理体系的建设，以及管理、技术和保障的相互结合。

12.3.1.4 建设原则

信息系统安全坚持“安全第一、预防为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，执行信息系统安全等级保护制度。

网络安全体系的建设，涉及面广、工作量大，必须坚持以下的原则，保证建设和运营的效果。

- **统一规划**

要对的网络安全体系建设进行统一的规划，制定网络安全体系框架，明确保障体系中所包含的内容。同时，还要制定统一的网络安全建设标准和管理规范，使得网络安全体系建设能够遵循一致的标准，管理能够遵循一致的规范。

- **分步有序实施**

网络安全体系的建设，内容庞杂，必须坚持分步骤的有序实施原则，循序渐进地进行。

- **基于安全需求**

依据信息系统担负的使命，积累的信息资产的重要性以及可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果。

- **技术管理并重**

仅有全面的安全技术和机制是远远不够的，安全管理也具有同样的重要性，西宁市人大常委会办公室信息系统网络安全体系的建设，必须遵循安全技术和

安全管理并重的原则。制定统一的安全建设管理规范，指导的安全管理工作。

- **突出安全保障**

网络安全体系建设要突出安全保障的重要性，通过数据备份、冗余设计、应急响应、安全审计、灾难恢复等安全保障机制，保障业务的持续性和数据的安全性。

- **持续改进**

信息系统安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进网络安全管理体系的有效性。

- **依法管理**

网络安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

- **自保护和国家监管结合**

对信息系统安全实行自保护和国家保护相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家网络安全。

12.3.1.5 建设目标

根据西宁市人大常委会办公室信息系统网络安全体系建设需求和原则，西宁市人大常委会办公室信息系统网络安全的建设目标，可以用“一个目标、两种手段、三个体系”进行概括。

- **一个目标**

西宁市人大常委会办公室信息系统网络安全的建设目标是：基于安全基础设施、以安全策略为指导，提供全面的安全服务内容，覆盖从物理、网络、系统、直至数据和应用平台各个层面，以及保护、检测、响应、恢复等各个环节，构建全面、完整、高效的网络安全体系，从而提高西宁市人大常委会办公室信

息系统信息系统的整体安全等级，为西宁市人大常委会办公室信息系统的业务发展提供坚实的网络安全保障。

- **两种手段**

网络安全体系的建设应该包括安全技术与安全管理两种手段，其中安全技术手段是安全保障的基础，安全管理手段是安全技术手段真正发挥效益的关键，管理措施的正确实施同时需要有技术手段来监管和验证，两者相辅相成，缺一不可。

- **三个体系**

西宁市人大常委会办公室信息系统网络安全体系的建设最终形成 3 个主要体系，具体包括安全技术体系、安全管理体系、以及运行保障体系。

12.3.2 安全体系框架

西宁市人大常委会办公室信息系统进行网络安全建设的目标是建立起一个全面、有效的网络安全体系，在这个体系中，包括了安全技术、安全管理、人员组织、教育培训、资金投入等关键因素，网络安全建设的内容多，规模大，

必须进行全面的统筹规划，明确网络安全建设的工作内容、技术标准、组织机构、管理规范、人员岗位配备、实施步骤、资金投入，才能够保证网络安全建设有序可控地进行，才能够使得网络安全体系发挥最优的保障效果。

12.3.2.1 网络安全需求

1.防火墙和网络边界保护：需要设置防火墙和网络边界保护设备，以阻止未授权的访问、内外网络之间的非法数据交换和恶意攻击。

2.身份认证和访问控制：需要确保用户的身份认证，限制未经授权的用户访问网络系统和数据，并设置访问权限和权限控制。

3.数据保密性和加密：对敏感信息进行加密传输和存储，保证数据在传输过程中不被窃取和篡改，确保数据的保密性。

4.防病毒和恶意软件：安装并定期更新防病毒和恶意软件软件，及时发现和清除病毒、恶意软件和木马程序，保证网络系统的安全。

5.安全审计和日志记录：建立安全审计和日志记录机制，记录用户的操作行为和网络事件，及时发现异常情况，追踪和分析安全事件，并采取相应的措施。

6.数据备份和恢复：定期对网络系统数据进行备份，确保系统数据的完整性和可用性，在系统发生故障或数据丢失时能够快速恢复。

12.3.2.2 安全模型

根据西宁市人大常委会办公室信息系统网络安全体系建设目标和总体安全策略，建立了与之对应的目标模型，称为 WP2DRR 安全模型，该模型是基于时间的，由预警（Warning）、策略（Policy）、保护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）六个要素环节构成了一个完整的、动态的网络安全体系。预警、保护、检测、响应、恢复等环节都由技术内容和管理内容所构成。



- Policy(安全策略)：根据风险分析和评估产生的安全策略描述了系统中哪些资源要得到保护，以及如何实现对它们的保护等。在WP2DRR 安全模型中，策略处于核心地位，所有的防护、检测、响应、恢复都依据安全策略展开实施，安全策略为安全管理提供管理方向和支持手段。

- Warining（预警）：根据以前所掌握的系统的弱点和当前了解的犯罪趋势预测未来可能受到的攻击和及危害。包括风险分析、病毒预报、黑客入侵趋势预报和情况通报、系统弱点报告和补丁到位。

- Protection（防护）：通过修复系统漏洞、正确设计开发和安装

安全系统来预防安全事件的发生；通过定期检查来发现可能存在的系统弱点；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监控等手段来防止恶意威胁。

- Detection（检测）：检测是非常重要的一个环节，检测是动态响应和加强防护的依据，它也是强制落实安全策略的有力工具，通过检测和监控网络和信息系统，发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。
- Response（响应）：响应是对安全事件做出反应，包括对检测到的系统异常或者攻击行为做出响应动作，以及处理突发的安全事件。恰当的响应动作和响应流程可以降低安全事件的不良影响，加强对重要资源的保护。
- Recovery（恢复）：灾难恢复能力直接决定了业务应用的持续可用性，任何意外的突发事件都可能造成服务中断和数据受损，优秀的灾难恢复计划能够针对灾难事件做到未雨绸缪，即使系统和数据遭受破

坏，也能够在最短的时间内，完成恢复操作。

WP2DRR 安全模型的特点就是动态性和基于时间的特性。它阐述了这样一个结论：安全的目标实际上就是尽可能地增大保护时间，尽量减少检测时间和响应时间。

WP2DRR 模型是在传统的 P2DR 模型的基础上新增加了预警 Warning 和恢复 Recover，增强了安全保障体系的事前预防和事后恢复能力，一旦系统安全事故发生了，也能恢复系统功能和数据，恢复系统的正常运行。

安全目标模型是网络安全体系框架的基础，西宁市人大常委会办公室信息系统的网络安全体系框架紧密围绕这个安全模型的 6 个要素环节进行设计，每个要素环节的功能都在安全技术体系、安全组织和管理体系以及运行保障体系中体现出来。

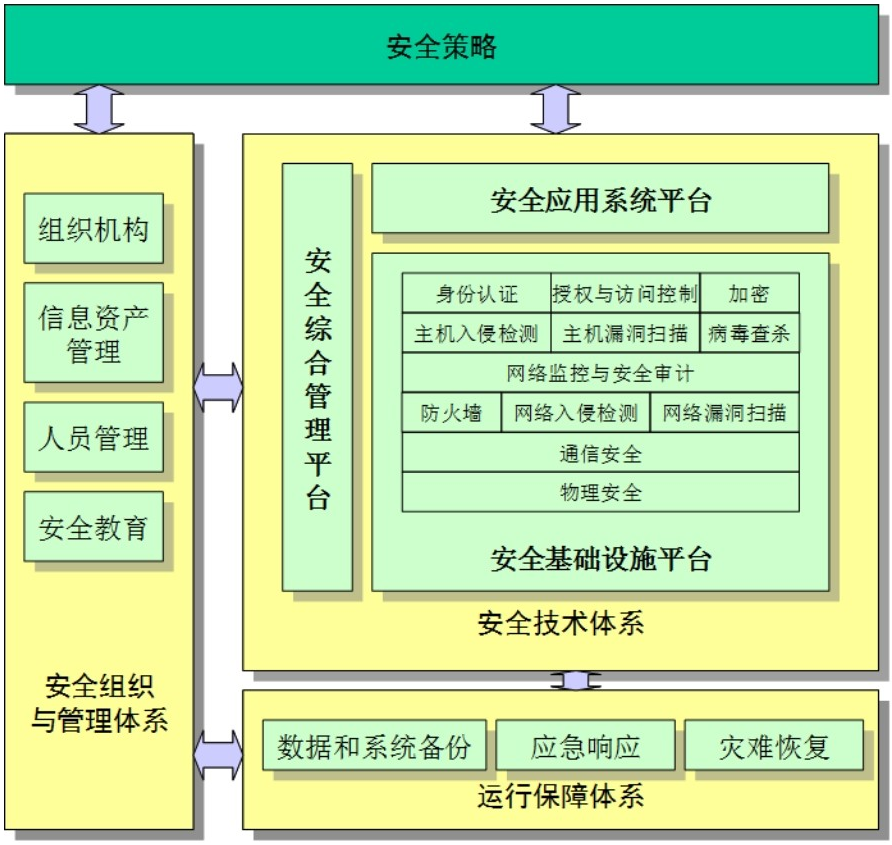
12.3.2.3 安全体系框架

通过对西宁市人大常委会办公室信息系统的网络和应用现状、安全现状、面临的安全风险的分析，根据安全保障目标模型，制定了西宁市人大常委会办公

室信息系统网络安全体系框架，制定该框架的目的在于从宏观上指导和管理网络安全体系的建设和运营。

该框架由一组相互关联、相互作用、相互弥补、相互推动、相互依赖、不可分割的网络安全保障要素组成。在此框架中，以安全策略为指导，融会了安全技术、安全管理和运行保障三个层次的安全体系，达到系统可用性、可控性、抗攻击性、完整性、保密性的安全目标。

西宁市人大常委会办公室信息系统网络安全体系框架的总体结构如下图所示：



- **安全策略**

在这个框架中，安全策略是指导。安全策略与安全技术体系、安全组织和管理体系以及运行保障体系这三大体系之间的关系也是相互作用的。一方面，三大体系是在安全策略的指导下构建的，主要是要将安全策略中制定的各个要素转化成为可行的技术实现方法和管理、运行保障手段，全面实现安全策略中所制定的目标；另一方面，安全策略本身也有包括草案设计、评审、实施、培训、部署、监控、强化、重新评估、修订等步骤在内的生命周期，需要采用一些技术方法和管理手段进行管理，保证安全策略的及时性和有效性。

- **安全技术体系**

安全技术体系是整个网络安全体系框架的基础，包括了安全基础设施平台、安全应用系统平台和安全综合管理平台这三个部分，以统一的网络安全基础设施平台为支撑，以统一的安全系统应用平台为辅助，在统一的综合安全管理平台管理下的技术保障体系框架。

安全基础设施平台是以安全策略为指导，从物理和通信安全防护，网络安全

防护，主机系统安全防护，应用安全防护等多个层次出发，立足于现有的成熟安全技术和安全机制，建立起的一个各个部分相互协同的完整的安全技术防护体系。

安全应用系统平台处理安全基础设施与应用信息系统之间的关联和集成问题，应用信息系统通过使用安全基础设施平台所提供的各类安全服务，提升自身的安全等级，以更加安全的方式，提供业务服务和内部信息管理服务。

安全综合管理平台的管理范围尽可能地涵盖安全技术体系中涉及的各种安全机制与安全设备，对这些安全机制和安全设备进行统一的管理和控制，负责管理和维护安全策略，配置管理相应的安全机制，确保这些安全技术与设施能够按照设计的要求协同运作，可靠运行。它在传统的信息系统应用体系与各类安全技术、安全产品、安全防御措施等安全手段之间搭起桥梁，使得各类安全手段能与现有的信息系统应用体系紧密的结合实现无缝连接，促成信息系统安全与信息系统应用的真正的一体化，使得传统的信息系统应用体系逐步过渡向安全的信息系统应用体系。

统一的安全管理平台有助于各种安全管理技术手段的相互补充和有效发挥，也便于从系统整体的角度来进行安全的监控和管理，从而提高安全管理工作的效率，使人为的安全管理活动参与量大幅下降。

- **安全管理体系**

安全组织和管理体系是安全技术体系真正有效发挥保护作用的重要保障，安全管理体系的设计立足于总体安全策略，并与安全技术体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷。

技术和管理是相互结合的，一方面，安全防护技术措施需要安全管理措施来加强，另一方面技术也是对管理措施贯彻执行的监督手段。在西宁市人大常委会办公室信息系统网络安全体系框架中，安全管理体系的设计充分参考和借鉴了国际网络安全管理标准《BS7799（ISO17799）》的建议要求。

西宁市人大常委会办公室信息系统网络安全管理体系由若干网络安全管理类组成，每项网络安全管理类可分解为多个安全目标和安全控制。每个安全目标都有若干安全控制与其相对应，这些安全控制是为了达成相应安全目标的管理

工作和要求。网络安全管理体系一共包括了 12 项管理类：

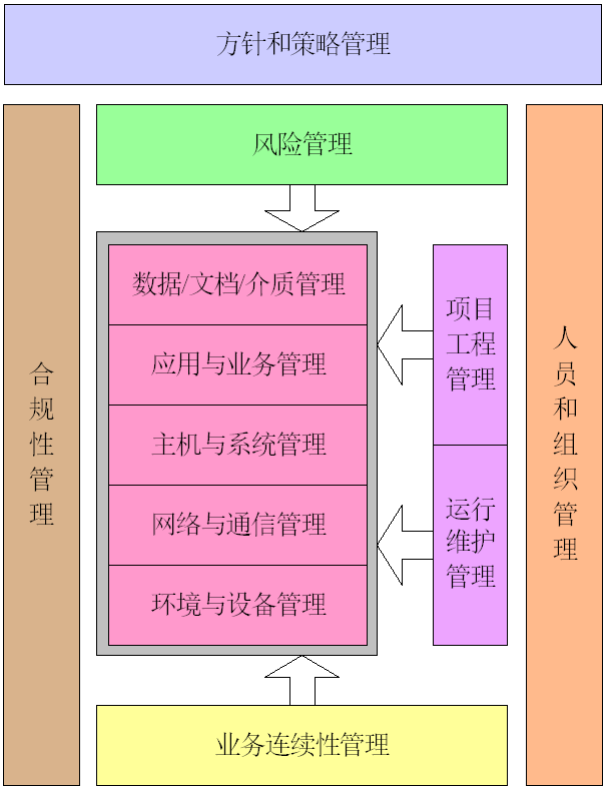
- 安全策略与制度，确保西宁市人大常委会办公室信息系统拥有明确的网络安全方针以及配套的策略和制度，以实现对网络安全工作的支持和承诺，保证网络安全的资金投入。
- 安全风险管理，网络安全建设不是避免风险的过程，而是管理风险的过程。没有绝对的安全，风险总是存在的。网络安全体系建设的目标就是要把风险控制在可以接受的范围之内。风险管理同时也是一个动态持续的过程。
- 人员和组织安全管理，建立组织机构，明确人员岗位职责，提供安全教育和培训，对第三方人员进行管理、协调网络安全监管部门与行内其它部门之间的关系，保证网络安全工作的人力资源要求，避免由于人员和组织上的错误产生的网络安全风险。
- 环境和设备安全管理，控制由于物理环境和硬件设施的不当所产生的风险。管理内容包括物理环境安全、设备安全、介质安全等。
- 网络和通信安全管理，控制和保护网络和通信系统，防止其受

到破坏和滥用，避免和降低由于网络和通信系统的问题对西宁市人大常委会办公室信息系统业务系统的损害。

- 主机和系统安全管理，控制和保护西宁市人大常委会办公室信息系统的计算机主机及其系统，防止其受到破坏和滥用，避免和降低由此对业务系统的损害。
- 应用和业务安全管理，对各类应用和业务系统进行安全管理，防止其收到破坏和滥用。
- 数据安全和加密管理，采用数据加密和完整性保护机制，防止数据被窃取和篡改，保护业务数据的安全。
- 项目工程安全管理，保护信息系统项目工程过程的安全，确保项目的成果是可靠的安全系统。
- 运行和维护安全管理，保护信息系统在运行期间的安全，并确保系统维护工作的安全。
- 业务连续性管理管理，通过设计和执行业务连续性计划，确保信息系统在任何灾难和攻击下，都能够保证业务的连续性。

- 合规性（符合性）管理，确保西宁市人大常委会办公室信息系统的网络安全保障工作符合国家法律、法规的要求；且西宁市人大常委会办公室信息系统的网络安全方针、规定和标准得到了遵循。

12 项网络安全管理类之间的关系，如下图所示。



12 项网络安全管理类的作用关系为：

- 方针和策略：是西宁市人大常委会办公室信息系统整个网络安全管理工作的基础和整体指导，对于其它所有的网络安全管理类都有指

导和约束关系。

- 人员和组织管理：是要依据方针和策略来执行网络安全管理工作。
- 合规性：指导如何检验网络安全管理工作的效果。特别是对于国家法律法规、方针政策和标准符合程度的检验。
- 根据“方针和策略”，由“人员和组织”实施网络安全管理工作。在实施中主要从两个角度来考虑问题，即风险管理和业务连续性管理。
- 根据信息系统的生命周期，可以将信息系统划分为两个阶段，即项目工程开发阶段和运行维护阶段。这两个网络安全管理类体现了信息系统和网络安全工作的生命周期特性。
- 最终所有的网络安全管理工作都作用在信息系统之上。信息系统可以划分成 5 个层次，从底层到上层依次为环境与设备管理、网络与通信管理、主机与系统管理、应用与业务管理、数据/文档/介质管理。这 5 个网络安全管理类体现了信息系统和网络安全工作的层次性。

- **运行保障体系**

运行与保障体系由安全技术和安全管理紧密结合的内容所组成，包括了系统可靠性设计、系统数据的备份计划、安全事件的应急响应计划、安全审计、灾难恢复计划等，运行和保障体系对于西宁市人大常委会办公室信息系统网络和信息系统的可持续性运营提供了重要的保障手段。

- **建设实施规划**

建设实施规划是在安全管理体系、安全技术体系、运行保障体系设计的基础上进一步制定的建设步骤和实施方案。在建设实施规划中突出体现了分步有序实施的原则。

任何网络安全建设都需要人员负责管理和实施，因此，首先应该建立网络安全网络和信息化安全领导小组，明确各级管理机构的人员配备，职能和责任。其中网络安全网络和信息化安全领导小组负责网络安全策略的审核与颁布、统一技术标准和管理规范的制定、指导和监督网络安全建设工作、对网络安全系统进行监控与审计管理。然后，对所有员工进行基本安全教育，为网络安全系

统相关技术人员提供专门的安全理论和安全技能培训，提高全员的安全意识，打造一支高素质的专业技术和管理队伍。

网络安全体系建设，应该首先从物理环境安全建设入手，确保机房建设按照的统一标准进行建设，并且按照统一的管理规范进行管理。

接下来应该进行网络安全建设，应该对计算机网络的安全域进行划分，对网络结构进行调整，确保内部网络与外部网络、业务网络与办公网络边界清晰；在各安全域的边界处部署防火墙、网络入侵检测等安全产品，形成立体的区域边界保护机制，对各安全域进行逻辑安全隔离，禁止未授权的网络访问；在内部网络中部署网络脆弱性分析工具，定期对内部网络进行检查，并采取措施及时弥补新发现的安全漏洞。

在进行网络安全建设的同时，可以进行系统安全建设，在内部网络中全面部署网络病毒查杀系统，有效抑制计算机病毒在内部网络中传播，避免对系统和数据造成损害；另外，主机系统管理员还应该按照主机系统管理规范的要求，借助主机脆弱性分析和安全加固工具，定期对主机系统进行检查，更新安全漏

洞补丁的级别，修正不当的系统和服务配置，查看和分析系统审计日志，控制和保证主机系统的良好安全状态。

应用安全建设包括建立身份认证系统、应用授权和访问控制系统、数据安全传输系统等，对业务应用系统和内部信息管理系统提供各种安全服务。

按照的统一标准，建立安全审计与分析系统、系统和数据备份计划、安全事件应急响应计划、灾难恢复计划等安全保障机制，重在保护业务数据等信息资产，保证内外应用服务的持续可用性。

12.3.3 运维内容

西宁市人大常委会办公室信息系统的网络安全建设所涉及的工作内容包括以下部分。

12.3.3.1 组织机构

建立专职的网络安全监管机构，明确各级管理机构的人员岗位配置和职能权限，全面负责网络安全建设工作和维护网络安全系统的运营。

12.3.3.2 人员管理

依据信息系统安全等级保护要求，对人员录用、考核、培训、离岗等一系列管理进行规范性要求。

制定统一的人员安全管理和教育培训规范，定期对信息系统的用户进行安全教育和培训，对普通用户进行基本的安全教育，对安全技术岗位的用户进行岗位技能培训，提高全员的安全意识，培养高素质的安全技术和管理队伍。

12.3.3.3 物理管理

按照国家对于计算机机房的相关建设标准，制定统一的计算机机房建设标准和管理规范，对于计算机机房建设中的环境参数、保障机制，以及运行过程中的人员访问控制、监控措施等进行统一约定，颁布统一的计算机机房管理制度，对设备安全管理、介质安全管理、人员安全管理等作出详细的规定。

12.3.3.4 网络管理

网络安全是信息安全保障的重点，制定统一的网络结构技术标准，对如何划

分内部信息系统的安全区域，安全区域的边界采取的隔离措施，进行约定，保证内部网络与外部网络、办公网与业务生产网之间的安全隔离。

制定统一的互联网接入点、外联网接入点的技术标准和管理规范，统一约定网络边界接入点的网络结构、安全产品的部署模式，保证内部网络与外部网络之间的安全隔离。

制定统一的网络安全系统建设标准和管理规范，包括防火墙、网络入侵检测、网络脆弱性分析、网络层加密等。

12.3.3.5 系统管理

系统安全的工作内容包括制定统一的系统安全管理规范，包括主机入侵检测、系统安全漏洞分析和加固， 提升服务器主机系统的安全级别。

制定统一的网络病毒查杀系统的建设标准和管理规范，有效抑制计算机病毒在内部网络和信息系统中的传播和蔓延。

12.3.3.6 应用管理

应用安全机制在应用层为业务系统提供直接的安全保护，能够满足身份认证、

用户授权与访问控制、数据安全传输等安全需求。

制定统一的身份认证、授权与访问控制、应用层通信加密等应用层安全系统的建设标准和管理规范，改善业务应用系统的整体安全性。

12.3.3.7 数据管理

系统数据备份是重要的安全保障机制，为了保障业务数据的安全性，降低突发意外事件所带来的安全风险，制定统一的系统和数据备份标准与规范，采取先进的数据备份技术，保证业务数据和系统软件的安全性。

12.3.3.8 运维管理

运维管理是在网络的基础设施建设完成之后，对运行环境（包括物理网络，软硬件环境等）、业务系统等进行维护管理。结合工作及信息化建设实际，建立运维管理标准及应用制度，采用标准的运维管理流程，完善系统运维管理体系，保证信息系统安全稳定的运行。

灾难是指对网络和信息系统造成任何破坏作用的意外事件，要制定详细的灾

难恢复计划，考虑到数据大集中的安全需求，采用异地容灾备份等技术，确保数据的安全性和业务的持续性，在灾难发生后，尽快完成恢复。

制定统一的应急响应计划标准，建立应急响应计划，包括安全事件的检测、报告、分析、追查、和系统恢复等内容。在发生安全事件后，尽快作出适当的响应，将安全事件的负面影响降至最低，保障业务正常运转。

12.3.4 总体安全解决策略

网络安全策略是网络安全建设的核心，它描述了在网络安全建设过程中，需要对哪些重要的信息资产进行保护，以及如何进行保护。

总体策略的设计坚持管理与技术并重的原则，以确保网络和信息系统的安全性为主，采用多重保护、最小授权、和严格管理等措施，从宏观整体的角度进行阐述，是网络安全建设总的指导原则。

12.3.4.1 物理环境安全解决策略

（1）计算机机房的建设必须遵循国家在计算机机房场地选择、环境安全、布

线施工方面的标准，保证物理环境安全。

（2）关键应用系统的服务器主机和前置机服务器、主要的网络设备必须放置于计算机机房内部的适当位置，通过物理访问控制机制，保证这些设备自身的安全性。

（3）应当建立人员出入访问控制机制，严格控制人员出入计算机机房和其它重要安全区域，访问控制机制还需要能够提供审计功能，便于检查和分析。

（4）进入机房的工作人员必须由安全管理员或机房管理员全程陪同。

（5）机房内部必须部署基础防护系统和设备，如电子门禁系统、监控报警系统、防雷设备、消防灭火系统、防水监控系统、温湿度控制系统、UPS 供电系统和电磁屏蔽设备。

（6）建立计算机机房管理制度，对设备安全管理、介质安全管理、人员出入访问控制管理等做出详细的规定。

（7）管理机构应当定期对计算机机房各项安全措施和安全管理制度的有效性和实施状况进行检查，发现问题，进行改进。

12.3.4.2 通信网络安全策略

1、网络架构

（1）应核查业务高峰时期一段时间内主要网络设备（如路由器、交换机和防火墙提供网络通信功能的设备 ）的 CPU 使用率和内存使用率是否满足需要（如主要网络设备近一年内的 CPU 负载值均低于 60%）并且网络设备从未出现过宕机情况；

（2）核查综合网管系统（如 AD，AC 等）各通信链路带宽是否满足高峰时段的业务流量需要（如：接入网络和核心网络带宽在业务高峰期占用低于 60%）；

（3）依据某种原则划分不同的网络区域；

（4）重要网络区域与其他网络区域之间采取可靠的技术隔离手段，如网闸、防火墙 和设备访问控制列表(ACL)等；

（5）主要网络设备、安全设备的硬件冗余和通信线路冗余。

2、通信传输

（1）数据传输过程中使用校验码技术或密码技术来保证其完整性。如：客户

端到服务器、服务器到服务器之间要使用 SSL 等通信；

（2）通信过程中对敏感信息字段或整个报文进行加密。使用加密设备对数据加密后传输。

12.3.4.3 区域边界安全策略

1、边界防护

（1）端口级访问控制：网络边界处部署访问控制设备，指定端口进行跨越边界的网络通信，该端口配置并启用了安全策略;

（2）控制非法联入内网、非法联入外网：

（3）无线和有线的边界应该有边界防护设备防护。

2、访问控制

（1）启用边界访问控制策略（网闸、防火墙、路由器和交换机等提供访问控制功能的设备）；

（2）防火墙对应用识别，并对应用的内容进行过滤。

3、入侵防范

（1）检测网络入侵行为（关键节点部署：入侵保护系统、入侵检测系统、抗APT 攻击、抗 DDoS 攻击和网络回溯等系统或设备。对内外部的网络攻击行为进行检测、防止或限制）

4、恶意代码和垃圾邮件防护

（1）关键网络节点处部署防恶意代码技术措施（ 防病毒网关和 UTM 等提供防恶意代码功能的设备或系统）；

（2）部署了防垃圾邮件设备或系统。

5、安全审计

（1）部署综合安全审计系统或类似功能的系统平台，对网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

（2）部署上网行为管理系统或综合安全审计系统 ，对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析 。

12.3.4.4 计算环境安全策略

（1）应当对关键服务器主机设备提供冗余设计，防止单点故障造成网络服务中断。

（2）应当建立主机弱点分析机制，发现和弥补系统软件中存在的不当配置和安全漏洞，及时进行自我完善。

（3）应当建立主机系统软件版本维护机制，及时升级系统版本和补丁程序版本，保持系统软件的最新状态。

（4）应当建立主机系统软件备份和恢复机制，在灾难事件发生之后，能够快速实现系统恢复。

（5）可以建立主机入侵检测机制，发现主机系统中的异常操作行为，以及对主机发起的攻击行为，并及时向管理员报警。

（6）应当指定专门的部门和人员，负责主机系统的管理维护。

（7）应当建立主机系统管理规范，包括系统软件版本管理、主机弱点分析、主机审计日志检查和分析、以及系统软件的备份和恢复等内容。

（8）应当建立桌面系统使用管理规范，约束和指导用户使用桌面系统，并对

其进行正确有效的配置和管理。

（9）管理机构应当定期对各项系统安全管理制度的有效性和实施状况进行检查，发现问题，进行改进。

（10）应用系统必须在登录时要求输入用户名和口令。登录应用系统必须进行两种或两种以上的复合身份验证（如用户名口令+Ukey 或用户名口令+IP 与 MAC 地址绑定方式）。

（11）应用系统中设置的用户都必须是唯一用户，不能名称相同，且不能出现多人使用同一账户的情况；应用系统必须开启登录失败处理功能；应用系统必须开启登录连接超时自动退出等措施。

（12）应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

（13）应用系统必须开启日志审计功能；应用系统存储用户信息的设备在销毁、修理或转其他用途时，必须清楚内部存储的信息。

（14）在业务系统主要应用服务器中采用硬件冗余技术，避免硬件的单点故障导致服务中断。

（15）综合考虑性能和管理等因素，采用先进的系统和数据备份技术，在范围内建立统一的系统和数据备份机制，防止数据出现逻辑损坏。

（16）业务应用数据和设备配置文档都必须进行备份，以便发生问题时进行恢复；数据备份至其他设备上时，必须使用专门的备份通道，保证数据传输的完整性；数据本机备份时应检测其完整性；数据备份时必须使用专业的备份设备和工具，在数据传输和数据存储时，都必须是加密传输和存储。

（17）建立灾难恢复计划，提供灾难恢复手段，在灾难事件发生之后，快速对被破坏的信息系统进行恢复。对人员进行灾难恢复培训，定期进行灾难恢复的模拟演练。

（18）应当建立专门岗位，负责用户权限管理，以及授权和访问控制系统的建设、运行、维护。

（19）建立日常数据备份管理制度，对备份周期和介质保管进行统一规定。

（20）应当建立全面网络病毒查杀机制，实现全网范围内的病毒防治，抑止病毒的传播。

12.3.4.5 安全管理中心策略

（1）配备集中系统和设备管理功能的工具或平台，系统或平台需要有三权分立（系统管理员、审计管理员、安全管理员），份角色通过管理工具或平台进行相关审计安全审计操作 。（运维堡垒机、SOC 平台、日志审计系统等）

（2）划分安全管理运维区，对分布在网络中的安全设备或安全组件进行集中管控。（堡垒机、SC 等）

（3）网络中是否划分单独的管理 VLAN 用于对安全设备或安全组件进行管理；使用独立的带外管理网络对安全设备或安全组件进行管理（如运维堡垒机等）；

（4）部署具备运行状态监测功能的系统或设备，能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测（ APM，堡垒机、综合网管系统等）；

（5）部署日志审计系统，日志保留 60 天以上且不间断；

（6）部署网络版防病毒系统和补丁统一更新系统对；

（7）部署安全感知平台对对网络中发生的各类安全事件进行识别、报警和分析；

（8）确保范围内统一使用了唯一确定的时钟源（如部署 NTP 时钟服务器）

12.3.5 应急预案

为妥善应对和处置本单位信息系统信息安全突发事件、确保信息系统正常运行，根据《网络安全事件应急预案》有关精神，结合本单位实际情况，特制定本应急预案。

适用范围：本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对我单位网络和信息系统或其中的数据造成危害、对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

12.3.5.1 应急组织机构及职责

西宁市人大常委会办公室信息系统网络安全工作网络和信息化安全领导小组及其办公室，负责对信息系统安全突发事件进行领导、预防、监测、报告和应急处置，及时向上级相关部门汇报情况，必要时与公安机关联系,获得必需的技

术支持。

12.3.5.2 应急处置工作原则

1、统一领导、规范管理。信息系统突发事件处置工作在党组的领导下，由办公室统一协调，遵照“统一领导、综合协调、各司其职”的原则协同配合、具体实施，完善应急工作体系和机制。

2、各网络安全小组成员单位、部门按照《网络安全工作网络和信息化安全领导小组》的职责分工，依据相关要求，明确责任，密切协同。

3、预防为主，加强监控。积极做好日常安全工作，提高应对突发网络与信息安全事件的能力。建立和完善信息安全监控体系，加强对网络与信息安全隐患的日常监测，重点监控网页是否被篡改、信息发布是否异常、信息系统运行是否异常等问题。

12.3.5.3 网络安全事件分级

网络安全事件分四级：特别重大事件、重大事件、较大事件和一般事件。

1、特别重大事件：包括重要网络、信息系统遭受严重损失，造成系统大面

积瘫痪，丧失业务处理能力；关键数据、敏感数据丢失；对国家安全、社会秩序、经济建设和公众利益造成严重威胁和影响的事件。

1、重大事件：包括重要网络、信息系统遭受严重损失，造成系统长时间中断或局部瘫痪，极大影响业务处理能力。对国家安全、社会秩序、经济建设和公众利益造成严重威胁和影响的事件。

2、较大事件：包括重要网络、信息系统遭受较大损失，明显影响业务处理能力。对国家安全、社会秩序、经济建设和公众利益造成比较严重威胁和影响的事件。

3、一般事件：包括对国家安全、社会秩序、经济建设和公众利益构成一定威胁和影响的事件。

12.3.5.4 监测与预警

信息系统应急响应流程主要分为：监测与预警、应急处置，故障修复、恢复运行、详细备案。

1、加强预警监测

严格按照“谁主管谁负责、谁运行谁负责”的要求，做好网络和信息系统运行的网络安全监测和预警预报工作。

2、预警研判与发布

多方将预警研判监测和预警分级信息文件下发至我单位网络安全管理岗位人员，由网络安全管理岗位人员组织网络技术岗位人员及时处置预警监测信息、文件要求，联系运维服务商进行应急处理，同时报送应急小组相关领导。

2、预警响应

特别重大网络安全事件预警：重要网络和信息系统遭受特别严重的损害，大面积瘫痪；敏感信息、关键数据丢失或被窃，对国家和社会构成特别严重威胁；以及其他对国家、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

重大网络安全事件预警：重要网络和信息系统遭受严重的损害，局部瘫痪、中断；敏感信息、关键数据丢失或被窃，对国家和社会构成严重威胁；以及其他对国家、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

较大网络安全事件预警：较大网络安全事件。重要网络和信息系统遭受较大的损害，系统运行效率低下；敏感信息、关键数据丢失或被窃，对国家和社会构成较严重威胁；以及其他对国家、社会秩序、经济建设和公众利益构成严重威胁、造成较严重影响的网络安全事件。

一般网络安全事件预警：一般网络安全事件。重要网络和信息系统遭受一般性损害；敏感信息、关键数据丢失或被窃，对国家和社会构成一定威胁；以及其他对国家、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

12.3.5.5 应急处置

1、事件报告

网络安全事件发生后，立即启动应急预案，实时处置并及时报送信息。网络安全管理岗位人员立即先期组织处置工作，控制事态，消除隐患，组织研判，保存证据，做好信息通报工作。同时向网络和信息化安全办公室上报事件发生，由网络和信息化安全领导小组组织研判后，报告省网信办。

1、应急响应

应急事件发生后，由单位网络管理网络和信息化安全领导小组实施应急指挥工作，网络和信息化安全领导小组办公室成员组成应急事件工作小组，负责应急处置和支援保障工作，小组成员保持 24 小时联络畅通。

应急预案启动后，网络安全管理岗位人员组织网络技术岗位人员根据网络安全事件的性质选择不同的处理手段，确保该事件造成的社会影响最小，同时，在实施应急预案处理措施的过程中出现的其他突发网络安全事件，应第一时间同时上报相关领导，并实施相应处理措施：

特别重大网络安全事件、重大网络安全事件警报：网络技术岗位人员通知网络服务商及时切断系统网络、关闭系统，隔离主机。同时网络安全管理岗位人员报告网络和信息化安全领导小组及其办公室负责人，同意后上报省网络安全应急办公室，请求协助问题排查、应急技术支撑。

较大网络安全事件、一般网络安全事件警报：网络安全管理岗位人员组织网络技术岗位人员联系系统供应商、网络运营商协助应急处理，如有重要情况则

由网络安全管理岗位人员报经单位领导同意后上报省网络安全应急办公室。

3、故障修复：网络技术岗位人员及时报告网络安全管理人员，并根据网络安全事件性质判断是否能自行处理，如果不能，网络技术岗位人员则在第一时间联系软硬件相关厂家和通讯运营商进行技术支持，涉密系统则联系省网络安全应急办公室进行协助处理消除故障。

4、恢复运行：问题处理后，网络安全管理岗位人员组织网络技术岗位人员先进行问题测试，测试通过后恢复运行；如果测试后问题还在，则继续进入故障处理步骤，直至该问题消除，并解除警报。

5、详细备案：网络安全管理岗位人员事后应对安全事件的处理过程予以总结并形成报告，其内容包括:导致事件的原因分析(尽量辨别其属于偶发事件还是必然事件)，事件造成的危害和恢复程度，是否存在遗留问题，以及相应的改进建议等。有关情况报西宁市人大常委会办公室信息系统（相关安全管理部门）。

六、调查与评估

1、日常管理

各部门、各单位应按职责做好网络安全事件日常预防工作，做好网络安全检

查、隐患排查、风险评估和备案工作，健全信息通报机制，采取措施，建设和避免网络安全事件的发生和危害，提高防范和应对能力。

2、宣传和培训

各部门、各单位应充分利用多种传播媒介和方式，积极开展有关法律、法规和政策的宣传工作，加强网络安全基本知识和技能的培训，提高防范意识及技能。

2、应急响应流程及时限承诺

我司为本项目设立 7×24 小时应急值守电话及项目负责人应急专线，接到甲方通知或平台告警后立即响应：一般问题 30 分钟内响应、2 小时内解决；涉及断网、页面篡改、病毒入侵、遭受攻击等紧急事件，15 分钟内响应、1 小时内提出处置方案并同步开展处置，重大事件由项目负责人赶赴现场配合甲方处置。

页面篡改事件：第一时间下线被篡改页面或切换至备份页面，完整保存篡改前后页面截图、访问日志与服务器日志等证据，排查入侵路径并封堵，完成系统加固与漏洞修复后，经甲方确认方可恢复上线，并在 24 小时内提交事件分析报告。

微信公众号及门户网站内容异常事件：发现信息发布差错或账号异常登录时，立即暂停相应渠道发布权限，核实并更正错误内容，必要时向平台申请处置；同步更换账号口令、启用双因素校验，排查操作终端安全隐患，形成事件记录报送甲方。

病毒与恶意程序事件：隔离受感染主机，使用防病毒软件全盘查杀，必要时重装系统并恢复备份数据，确认无残留后恢复业务，同时核查同网段其他主机安全状况。

断网与网络攻击事件：配合网络运营商及安全厂商快速定位链路故障或攻击来源，启用备用链路或调整防护策略，控制影响范围，业务恢复后再组织一次安全自查。

上述应急处置全过程形成书面记录与总结报告，纳入年度运维报告及服务考核内容。

3、重要敏感时期网络安全应对措施

网络安全人员连同运营维护商在重要敏感时期进行 24 小时应急值班，对网络和信息数据加强保护，进行不间断监控，一旦发生网络与信息安全事件，立即

启动应急预案，判定事件危害程度，采取应急处置措施，并立即将情况报告有关领导。在处置过程中，及时报告处置工作进展情况，直至处置工作结束。属于重大事件或存在非法犯罪行为的，及时向公安机关报告。

12.4 本地化服务能力

本地化服务能力承诺函

致：西宁市人民代表大会常务委员会办公室

针对本项目本地化服务能力的要求，我方在此作如下承诺：

若我方中标，我方将在西宁市成立人大运维服务办事处，提供 5*8 小时服务热线，30 分钟上门、2 小时解决问题的服务保障能力，并提供 400 客户热线及 7*24 小时的项目负责人应急专线服务。

磋商响应单位：六合远教（成都）科技有限公司（公章）

2026 年 10 月 10 日

12.5 关于招标文件服务要求的响应

12.5.1 网络优化检测服务

我司承诺完全响应本项目的服务要求及指标：

（1）. 保障平台平稳安全运行，随时监控硬件以及软件使用情况。

（2）. 采用软件自动化实时对硬件进行检测服务，合理分析硬件使用情况后在做出最优规划。

（3）. 软件优化检测服务，通过人工配合优化监测软件完成，通过对软件参数设置取得的使用效果，测试软件承受范围内达到最高性能负载。根据测试数据，调整、优化软件建设规划。

（4）. 结合硬件与软件检测报告，统计分析数据，逐步优化完善人大代表网络履职平台。

12.5.2 平台计算资源维护

我司承诺完全响应本项目的服务要求及指标：

（1）．保证平台硬件设备长期、正常运转，需要对服务器和相关设备的统计和标记工作；定时检查和保障服务器的维护工作，包括系统安装，系统补丁更新；对网络故障进行判断和排查。对服务器

（2）．使用安全措施处理包括但不限于 DDOS 攻击在内的系统安全问题。

（3）．定期测试系统安全性，根据现有系统架构规划、调整安全防护措施。

（4）．实时的对网络流量进行监控，处理异常问题。

12.5.3 平台软件维护

我司承诺完全响应本项目的服务要求及指标：

（1）．根据《中华人民共和国网络安全法》要求，服务器主机、应用平台软件应满足《信息安全技术网络安全等级保护基本要求》第三级安全要求（以下简称“等保三级”），对不满足等保三级标准的，及时发现，及时整改。

（2）．配合甲方进行等保三级测评工作。包括但不限于甲方需建立安全管理制度、方案编写等工作的情况；对测评过程中需要乙方提供包括但不

限于文字资料、技术支持的情况。

（3）． 在使用过程中对系统程序本身、中间件、数据库、数据等进行维护保证平台正常运行。对程序本身、操作系统、中间件、数据库出现漏洞的，需及时修复。漏洞来源包括但不限于国家、省、市网信或公安部门发布、平台涉及软件所属厂家发布、国内外知名安全厂家发布、乙方上级部门通知，甲方通知。

（4）．定时完成对系统程序、数据库进行备份、恢复、临时数据统计分析。

（5）．根据网站优化检测结果对网站进行持续优化，提出优化方案。

（6）．对西宁人大平台进行持续的优化和维护升级。

（7）．平台内无效或者问题链接定期处理，并对平台的网络安全进行防护做出相关措施。

12.5.4 页面分布及内容修改

我司承诺完全响应本项目的服务要求及指标：

（1）．采用技术措施全年完成至少一次全站内容安全检测，每篇信息发布前采用技术措施进行内容安全检测，确保信息发布准确无误。

（2）．根据甲方的要求对页面分布、数据、内容进行适当调整。

（3）．根据甲方的需要，建设 1-2 个专题栏目。

12.5.5 微信公众号及门户网站信息发布

我司承诺完全响应本项目的服务要求及指标：

（1）．根据甲方需求，负责“西宁人大”微信公众号的日常内容更新与维护、负责西宁人大门户网站的内容更新与维护，发布前进行人工复审，确保信息发布准确无误。

12.5.6 培训

我司承诺完全响应本项目的服务要求及指标：

针对甲方业务操作人员、技术维护人员运维服务期内进行不少于一次业务、技术及安全培训。

12.6 关于商务要求的承诺

商务要求承诺函

致：西宁市人民代表大会常务委员会办公室

我司针对本项目商务部分要求，承诺如下：

1、服务期：按合同约定执行。

2、服务地点：采购人指定地点。

3、付款方式：按合同约定执行。

磋商响应单位：六合远教（成都）科技有限公司（公章）

2026 年 10 月 10 日

12.7　不存在其他实质性偏离情况的承诺

商务要求响应承诺函

致：西宁市人民代表大会常务委员会办公室

我司承诺不存在如下他实质性偏离情况：

（1）不符合第 2.2 款“合格的供应商”之规定的；

（2）未按第 10.1 款（1）-（13）要求提供相关资料的；

（3）响应文件内容没有按磋商文件规定和要求签字、盖章的；

（4）响应文件编排混乱，且擅自修改磋商文件规定的格式内容的；

（5）交货时间、磋商有效期不能满足磋商文件要求的；

（6）产品的技术规格、技术标准明显不符合采购项目要求的；

（7）响应文件中附有采购人不能接受的条件的；

（8）报价超过采购预算额度的；

（9）磋商小组认为应按无效响应处理的其他情况；

（10）法律、法规规定的其他情形。

同时我司非联合体方式参与本项目，也不存在磋商文件中规定的其他资质条件不满足的情况。

磋商响应单位：六合远教（成都）科技有限公司（公章）

2026 年 10 月 10 日

13 最终报价表

最终磋商报价表

供应商名称（盖章）：　　日期：　年　月　日

项目名称	最后磋商总价（人民币：元）	服务期	备注
	大写：		
	小写：		
最终确定的服务承诺：			

注：此表不需装订在磋商响应文件中，供应商事先须盖章、签字。在磋商期间，

由磋商小组确定合格的供应商按要求现场填写。

磋商响应单位： 六合远教（成都）科技有限公司 （公章）

法定代表人或委托代理人：（签字或盖章） 年 月 日