

二、 投标报价一览表

2.1 投标报价一览表

供应商名称	中国联合网络通信有限公司漯河分公司
项目名称	濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目 第二标包
投标总报价（人民币）	大写： 贰佰伍拾贰万壹仟陆佰元整 小写： 2521600 元
投标有效期	自投标截止之日起90日历天
服务期限	合同签订后15日历天完成
质量要求	满足国家相关法律规定和现行行业标准与规范和招标文件要求
备注	满足招标文件的其他要求

供应商名称（盖单位公章）：中国联合网络通信有限公司漯河分公司

法定代表人或授权委托人（签字）：

2024 年 4 月 9 日

2.2 附件：技术偏差表

序号	采购文件章节及条款号	响应文件章节及条款号	偏差说明
1	第二章2.1总体要求 供应商负责建设电子政务外网骨干线路，并提供相应设备。供应商负责满足省市电子外网对接规范，上联省级电子政务外网，横向兼容其他供应商骨干网络。供应商负责提供电子政务外网核心标准机房，该机房由电子政务外网管理机构管理使用，供应商负责进行维护。供应商提供电子政务外网线路多速率带宽服务供使用方选择。供应商为市级核心节点提供千兆互联网带宽服务，线路需支持IPv6协议，并提供不少于一个1C的互联网IP。 1. 网络互联互通的需求 电子政务网平台建立后，应在纵向上实现上连国家、省、市电子政务外网平台，下连各乡镇电子政务外网平台，在横向上能够方便连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等。同时，网络必须具备高度的可靠性和稳定性，应具备可伸缩、可管理、可扩展的能力，以应对业务数据的快速增长，满足网络平台平滑升级的要求。 2. 互联网接入的需求 外网平台应能够提供整个网络统一的安全的互联网接入。 3. IPV6升级 供应商建设的电子政务外网需支持国家关于电子政务外网IPV6升级的基本需求。	第一章11.1 我方负责建设电子政务外网骨干线路并提供相应设备。我方负责满足省市电子外网对接规范，上联省级电子政务外网，横向兼容其他我方骨干网络。我方负责提供电子政务外网核心标准机房，该机房由电子政务外网管理机构管理使用，我方负责进行维护。我方提供电子政务外网线路多速率带宽服务供使用方选择。我方为市级核心节点提供千兆互联网带宽服务，线路需支持IPv6协议，并提供不少于一个1C的互联网IP地址。 1. 网络互联互通的需求 电子政务网平台建立后，能够在纵向上实现上连国家、省、市电子政务外网平台，下连各乡镇电子政务外网平台，在横向上能够方便连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等。同时，电子政务网络具备高度的可靠性和稳定性，具备可伸缩、可管理、可扩展的能力，能够满足应对业务数据的快速增长，满足网络平台平滑升级的要求。 2. 互联网接入的需求 外网平台能够提供整个网络统一的安全的互联网接入。 3. IPV6升级	无偏离

	4. 政务云对接需求 供应商建设的电子政务外网须实现互联互通，并对接本地现有政务云，并实现政务系统互联互通。	我方建设的电子政务外网能够支持国家关于电子政务外网IPv6升级的基本要求。 4. 政务云对接需求 我方建设的电子政务外网能够实现互联互通，并对接本地现有政务云，并实现政务系统互联互通。	
2	第二章2.2管理要求。 采购人负责政务外网的统筹管理，并按照统一规划、统筹管理、平均分配的原则，分配政务外网IP地址。 供应商负责端到端的物理设备及链路的故障定位和排除、管理设备配置。未经采购方许可，所有设备不可与其它网络并用，从物理到逻辑均为单一独立的局域网络。供应商明确一个负责人或团队对电子政务外网线路进行运行维护，因特殊原因需更换负责人或团队，应及时告知电子政务外网管理机构。供应商需提供网络运维管理、安全监测服务，并交于采购方使用； 1. 传输质量要求。 供应商提供的线路需满足以下条件：默认PING传输时延上限值为10ms；PING带2000字节包，上限值为20ms；（省市设备间延时上限值为100ms；市县设备间延时上限值为50ms） 2. 故障处置。 供应商应提供7×24小时呼叫服务专线；从用户报障开始计算人员，到场时间≤1小时，故障恢复时限≤4小时。除不可抗力及市政施工等原因以外，一年内发生不超过5次线路故障在48小时内未能及时修复。	第十一章11.2 濮阳市行政审批和政务信息管理局负责政务外网的统筹管理，并按照统一规划、统筹管理、平均分配的原则，分配政务外网IP地址。 若我方中标，我方将负责端到端的物理设备及链路的故障定位和排除、管理设备配置。未经濮阳市行政审批和政务信息管理局许可，所有设备不可与其它网络并用，从物理到逻辑均为单一独立的局域网络。我方将明确一个负责人和团队对电子政务外网线路进行运行维护，因特殊原因需更换负责人或团队，将及时告知电子政务外网管理机构。我方提供网络运维管理、安全监测服务，并交于濮阳市行政审批和政务信息管理局使用； 1. 传输质量要求 我方提供的线路将满足以下条件：默认PING传输时延上限值为10ms；PING带2000字节包，上限值为20ms；（省市设备间延时上限值为100ms；市县设备间延时上限值为50ms） 2. 故障处置 提供7×24小时呼叫服务专线；从用户报障开始计算人员，到场时间小于1小时，故障恢复时限小于4小时。除	无偏离

	3.日常巡检。 供应商必须建立光纤巡查机制。派专人就提供的光纤运行质量状态进行巡查。每季度巡查不少于一次，并做好巡查登记记录和通知维修记录。	不可抗力及市政施工等原因以外，一年内发生不超过5次线路故障在48小时内未能及时修复。 日常巡检 建立光纤巡查机制，派专人就提供的光纤运行质量状态进行巡查。每季度巡查一次，并做好巡查登记记录和通知维修记录。	
3	第二章2.3保密要求。 供应商提供的线路或相关工作人员应遵守保密原则，保证政务信息不因线路问题外泄。	第十一章11.4 保密要求。我方提供的线路或相关工作人员遵守保密原则，保证政务信息不因线路问题外泄。	无偏离
4	第二章2.4网络安全要求 供应商需对政务外网网络安全负责，所建设政务外网必须符合三级等保要求，并通过国家三级等保认证。供应商需采取必要的技术和管理措施，确保政务外网安全。	第十一章11.3.7.3网络安全要求 我方对政务外网网络安全负责，所建设政务外网符合信息安全三级等级保护要求，并通过国家三级等保认证，证书详见7.13章节。若我方中标，定会采取必要的技术和管理措施，确保政务外网安全。	无偏离
5	第二章2.5.1政策依据 (1)《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号） (2)《国家发展改革委关于印发〈“十四五”推进国家政务信息化规划〉的通知》（发改高技〔2021〕1898号） (3)中央网络安全和信息化委员会印发的《“十四五”国家信息化规划》 (4)《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102号） (5)《国务院办公厅关于加快推进政务服	第十一章11.3.10政策依据 (1)《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号） (2)《国家发展改革委关于印发〈“十四五”推进国家政务信息化规划〉的通知》（发改高技〔2021〕1898号） (3)中央网络安全和信息化委员会印发的《“十四五”国家信息化规划》 (4)《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102号）	无偏离

务“跨省通办”的指导意见》（国办发〔2020〕35号） (6)《中央网信办、国家发展改革委、工业和信息化部关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（中网办发〔2021〕15号） (7)《工业和信息化部 中央网络安全和信息化委员会办公室关于印发〈IPv6流量提升三年专项行动计划（2021-2023年）〉的通知》（工信部联通信〔2021〕84号） (8)《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》 (9)《河南省人民政府关于印发河南省“十四五”数字经济和信息化发展规划的通知》（豫政〔2021〕51号） (10)《河南省人民政府关于印发河南省加强数字政府建设实施方案（2023—2025年）的通知》（豫政〔2023〕17号） (11)《河南省人民政府办公厅关于印发河南省建立健全政务数据共享协调机制加快推进数据有序共享实施方案的通知》（豫政办〔2022〕62号） (12)《河南省人民政府办公厅关于加快推进新型智慧城市建设的指导意见》（豫政办〔2020〕27号） (13)《河南省推进互联网协议第六版（IPv6）规模部署实施计划》 (14)《濮阳市国民经济和社会发展第十四个五年发展规划和2035年远景发展目标纲要》	(5)《国务院办公厅关于加快推进政务服务“跨省通办”的指导意见》（国办发〔2020〕35号） (6)《中央网信办、国家发展改革委、工业和信息化部关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（中网办发〔2021〕15号） (7)《工业和信息化部 中央网络安全和信息化委员会办公室关于印发〈IPv6流量提升三年专项行动计划（2021-2023年）〉的通知》（工信部联通信〔2021〕84号） (8)《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》 (9)《河南省人民政府关于印发河南省“十四五”数字经济和信息化发展规划的通知》（豫政〔2021〕51号） (10)《河南省人民政府关于印发河南省加强数字政府建设实施方案（2023—2025年）的通知》（豫政〔2023〕17号） (11)《河南省人民政府办公厅关于印发河南省建立健全政务数据共享协调机制加快推进数据有序共享实施方案的通知》（豫政办〔2022〕62号） (12)《河南省人民政府办公厅关于加快推进新型智慧城市建设的指导意见》（豫政办〔2020〕27号） (13)《河南省推进互联网协议第六版（IPv6）规模部署实施计划》 (14)《濮阳市国民经济和社会发展第十四个五年发展规划和2035年远景发展目标纲要》
---	--

6	第二章2.5.2技术标准 (1)《中华人民共和国网络安全法》； (2)《中华人民共和国个人信息保护法》； (3)《中华人民共和国密码法》； (4)《中华人民共和国数据安全法》； (5)《关键信息基础设施安全保护条例》(国令第745号)； (6)《电子政务外网安全接入技术规范》(DB34/T 4283-2022)； (7)《国家电子政务外网IPv6地址规划》(GW0209—2019)； (8)《信息安全技术 网络安全等级保护测评要求》(GBT28448 -2019)； (9)《国家政务服务平台安全接入检测要求》(C0115-2018)； (10)《政务网络安全监测平台总体技术要求》(TCIIA 005-2019)； (11)《政务网络安全监测平台数据总线结构规范》(T/CIIA 007—2020)； (12)《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019)； (13)《信息安全技术网络安全等级保护安全设计技术要求》(GB/T 25070-2019)； (14)《信息安全技术网络安全等级保护实施指南》(GB/T 25058-2019)； (15)《信息安全技术网络安全监测基本要求与实施指南》(BG/T36635-2018)； (16)《信息安全技术 电子政务移动办公系统安全技术规范》(GB/T 35282-2017)； (17)《国家电子政务外网信息安全标准体系框架》(GW0101-2014)； (18)《国家电子政务外网信息安全标准化	第十一章11.3.11技术标准 (1)《中华人民共和国网络安全法》； (2)《中华人民共和国个人信息保护法》； (3)《中华人民共和国密码法》； (4)《中华人民共和国数据安全法》； (5)《关键信息基础设施安全保护条例》(国令第745号)； (6)《电子政务外网安全接入技术规范》(DB34/T 4283-2022)； (7)《国家电子政务外网IPv6地址规划》(GW0209—2019)； (8)《信息安全技术 网络安全等级保护测评要求》(GBT28448 -2019)； (9)《国家政务服务平台安全接入检测要求》(C0115-2018)； (10)《政务网络安全监测平台总体技术要求》(TCIIA 005-2019)； (11)《政务网络安全监测平台数据总线结构规范》(T/CIIA 007—2020)； (12)《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019)； (13)《信息安全技术网络安全等级保护安全设计技术要求》(GB/T 25070-2019)； (14)《信息安全技术网络安全等级保护实施指南》(GB/T 25058-2019)； (15)《信息安全技术网络安全监测基本要求与实施指南》(BG/T36635-2018)；	无偏离

	工作规范》(GW0102-2014)； (19)《接入政务外网的局域网安全技术规范》(GW0206-2014)； (20)《国家电子政务外网安全接入平台技术规范》(GW0202-2014)； (21)《国家电子政务外网安全管理系统技术要求与接口规范》(GW0204-2014)； (22)《国家电子政务外网安全等级保护实施指南》(GW0104-2014)； (23)《国家电子政务外网跨网数据安全交换技术要求与实施指南》(GW0205-2014)； (24)《国家电子政务外网安全监测体系技术规范与实施指南》(GW0203-2014)；	(16)《信息安全技术 电子政务移动办公系统安全技术规范》(GB/T 35282-2017)； (17)《国家电子政务外网信息安全标准体系框架》(GW0101-2014)； (18)《国家电子政务外网信息安全标准工作规范》(GW0102-2014)； (19)《接入政务外网的局域网安全技术规范》(GW0206-2014)； (20)《国家电子政务外网安全接入平台技术规范》(GW0202-2014)； (21)《国家电子政务外网安全管理系统技术要求与接口规范》(GW0204-2014)； (22)《国家电子政务外网安全等级保护实施指南》(GW0104-2014)； (23)《国家电子政务外网跨网数据安全交换技术要求与实施指南》(GW0205-2014)； (24)《国家电子政务外网安全监测体系技术规范与实施指南》(GW0203-2014)；	
7	第二章2.6采购内容参数要求 1、单条宽带$\geq 100\text{M}$； 2、速率要求上行、下行对称； 3、所提供的物理链接光纤信号衰减不超过20db； 4、采用专线直连的方式。	第十一章11.5.1采购内容参数响应 1、单条宽带100M； 2、速率上行下行对称； 3、提供的物理连接光纤信号衰减不超过20db； 4、采用专线直连的方式。	无偏离
8	第二章2.7建设工期及进度要求 合同签订后，要求在 15 天内完成。	第十一章11.5.2建设工期及进度要求 合同签订后，我方在15天内完成。	无偏离

9	第二章2.8售后运维要求 应制定系统运行维护计划、工作流程、管理制度、服务质量要求，应根据不同的联网系统设备、环境制定具体的保养方案。包括但不限于符合以下要求。（1）网络租赁维护期内，中标方对于系统故障应在1小时内响应，在2小时内确定故障原因和解决方案，在12小时内排除故障，24小时内不能修复的，保证线路稳定运行。 （2）中标人应配备不少于6人的专职运行维护、售后服务队伍。 （3）应制定系统日常维护工作计划，并严格按照工作计划进行系统的日常维护。日常维护不应影响系统的正常使用。 （4）招标方要求的其他内容，具体以后期合同约定。	第十一章11.7.8售后运维服务承诺 （1）网络租赁维护期内，若我方中标，我方将对于系统故障在1小时内响应，在2小时内确定故障原因和解决方案，在12小时内排除故障，24小时内不能修复的，保证线路稳定运行。 （2）我方配备10人的专职运行维护、售后服务队伍。 （3）制定系统日常维护工作计划，并严格按照工作计划进行系统的日常维护。日常维护不影响系统的正常使用。 （4）招标方要求的其他内容，具体以后期合同约定，我方满足。	无偏离
---	---	--	-----

注：

1. 供应商需按文件第二章要求应答，列出所投服务的具体应答。偏差说明一栏中对偏差予以详细说明（“正偏离”“无偏离”或“负偏离”）。
2. 投标者可根据其投标内容进一步细化上述表格，并可增添其它表格或说明以便进一步明确投标内容。

供应商名称(盖单位章):  中国联合网络通信有限公司濮阳市分公司

法定代表人或其委托代理人(签字): 

日期: 2024年4月9日



十、技术方案及服务方案

10.1 项目总体要求

我方负责建设电子政务外网骨干线路，提供网络设备。我方负责满足省市电子外网对接规范，上联省级电子政务外网，横向兼容其他我方骨干网络。我方负责提供电子政务外网核心标准机房，该机房由电子政务外网管理机构管理使用，我方负责进行维护。我方提供电子政务外网线路多速率带宽服务供使用方选择。我方为市级核心节点提供千兆互联网带宽服务，线路支持IPv6协议，并提供不少于一个1C的互联网IP地址。

1. 网络互联互通的需求

电子政务网平台建立后，能够在纵向上实现上连国家、省、市电子政务外网平台，下连各乡镇电子政务外网平台，在横向上能够方便连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等。同时，电子政务网络具备高度的可靠性和稳定性，具备可伸缩、可管理、可扩展的能力，能够满足应对业务数据的快速增长，满足网络平台平滑升级的要求。

2. 互联网接入的需求

外网平台能够提供整个网络统一的安全的互联网接入。

3. IPV6升级

我方建设的电子政务外网能够支持国家关于电子政务外网IPV6升级的基本需求。

4. 政务云对接需求

我方建设的电子政务外网能够实现互联互通，并对接本地现有政务云，并实现政务系统互联互通。

10.2 项目管理要求

濮阳市行政审批和政务信息管理局负责政务外网的统筹管理，并按照统一规划、统筹管理、平均分配的原则，分配政务外网IP地址。

若我方中标，我方将负责端到端的物理设备及链路的故障定位和排除、管理设备配置。未经濮阳市行政审批和政务信息管理局许可，所有设备不可与其它网络并用，从物理到逻辑均为单一独立的局域网络。我方将明确一个负责人和团队对电子政务外网线路进行运行维护，因特殊原因需更换负责人或团队，将及时告知电子政务外网管理机构。我方提供网络运维管理、安全监测服务，并交于濮阳市行政审批和政务信息

管理局使用；

1. 传输质量要求

我方提供的线路满足以下条件：默认带宽传输时延上限值为10ms；PING带2000字节包，上限值为20ms；（省市设备间延时上限值为30ms；市县设备间延时上限值为50ms）

2. 故障处置

提供7×24小时呼叫服务专线；从用户报障开始计算人员，到场时间小于1小时，故障恢复时限小于4小时。除不可抗力、市政施工等原因以外，一年内发生不超过5次线路故障在48小时内未能及时修复。

3. 日常巡检

建立光纤巡查机制。派专人就提供的光纤运行质量状态进行巡查。每季度巡查一次，并做好巡查登记记录和通知维修记录。

10.3 实施方案

10.3.1 建设目标

按照濮阳市行政审批和政务信息管理局电子政务外网规划部署，在充分利用现有电子政务资源的基础上，通过建设电子政务外网平台、运维支撑平台、安全防护体系、相关标准规范制度、机房环境等，为濮阳市行政审批和政务信息管理局和各政府单位电子政务外网平台之间建立公共非涉密信息传输通道，为各级政务部门实现互联互通、数据传输、资源共享、业务协同提供网络支撑环境，满足各级政务部门业务办公、社会管理和公共服务的需要，全面提高濮阳市政府单位电子政务水平。

10.3.2 需求分析

10.3.2.1 系统功能指标

1. 基础网络平台

濮阳市行政审批和政务信息管理局电子政务外网是濮阳市电子政务外网重要组成部分，其基础网络平台包括平台端局域网及单位接入网。网络平台为树形结构，平台端局域网部署在政务外网接入节点，单位接入网横向接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等，实现本级政务部门之间互联互通、信息交换和业务协同。为濮阳市政务部门提供安全、可控的互联网访问，同时实现互联网数据流与政务外网数据流进行有效的逻辑隔离保护政务外网不会因来自互联网拒绝服务攻击而瘫痪，对进出各安全域的信息和数据进行严格的控制，防止

对安全域的非访问，建设统一互联网出口，满足政府部门访问互联网需要。

2. 安全防护

按照信息安全等级保护三级要求，部署防火墙、安全审计系统、入侵检测系统等设备进行安全隔离和访问控制，保证电子政务外网数据传输安全，减少数据被窃听和篡改的可能；通过对服务器的备份系统、备份以及仲裁管理，保障系统的可控性；同时依靠门禁系统，防止非法用户进入计算机控制室和各种偷窃、破坏活动的发生。巩固濮阳市行政审批和政务信息管理局电子政务外网项目的安全支撑能力，满足安全等级保护的要求。

10.3.2.2 系统性能指标

1. 网络平台

我方提供数据传输网络畅通、快捷、安全、可扩展，能满足数据、图像、视频等传输要求。采用 MPLS VPN 与国家骨干网协同实现政务部门系统内业务专网的“中央-自治区-市-县-乡镇”五级网络贯通。能够适应电子政务网络业务增长的需求，确保系统的可扩展性和先进性，并注意设备的冗余设计以及网络的负载均衡及具备极强网络安全，为各级政务部门提供安全、可控的互联网访问，同时实现互联网数据流与政务外网数据流的有效隔离。

2. 专线电路

专线电路由我方提供，组成政务外网的基础线路。上层网络设备通过专线电路构建城域网基础，承载政务数据和业务应用传输交换。随着业务量逐渐增加能不断地扩充网络带宽，能实施相应网络带宽和服务质量保障策略，保证承载业务的顺畅运行。

3. 安全防护

本项目按照信息安全等级保护三级要求，分别建立边界安全防护措施，系统采用的安全产品应该通过国家相关部门的鉴定或认证，主要的安全建设如下：

- (1) 对信息系统的物理支撑环境进行安全设施部署，保障物理安全；
- (2) 对数据传输的基础网络进行安全设施部署，保障网络安全；
- (3) 对应用数据和基础数据提供行为审计、备份等安全设施部署，保障数据安全。

4. 机房及配套基础设施

机房是电子信息设备运转必须的基础设施环境条件，在统一规划的原则下充分满足电子政务外网系统运行的需要，达到方便维护，迅速响应，灵活扩充的目的。

10.3.3 总体设计原则

10.3.3.1 安全性原则

政务外网是濮阳市电子政务系统内部使用的计算机互联网络，其联网范围大，联接节点多，所以确保安全至关重要。为此在规划设计的全过程中要充分体现系统建设和信息安全相结合的原则，从物理、技术、管理等方面制定严密的安全方案，形成多层次、全方位的安全防线。

10.3.3.2 实用性原则

政务外网的建设，要充分体现系统的实用性。首先考虑已建网络或应用系统需求和特点，外网要兼容已有网络和系统；其次根据对各政务部门的业务需求进行调查，根据其调查的汇总需求，适当考虑其设备、技术的前瞻性，采用成熟的各种技术手段，实现各种功能，满足其政务部门的业务要求；再者充分考虑政务业务的特点，以及外网用户对使用方面的习惯、功能等要求，满足未来用户可能提出的要求。

10.3.3.3 先进性原则

政务外网作为通信手段，在网络方面要求具备先进的技术水平，以保证当前及今后一段时间内的各类应用顺利运行。由于网络设备及技术更新换代频繁，盲目的追求系统的先进性也会带来更大投资风险，因此在规划、设计外网时，既要考虑到先进性，同时避免盲目的投资风险，在网络设备上，具有一定的扩展性和兼容性，在技术上，保证三年内基本不过时。

10.3.3.4 可靠性原则

政务外网要求高度的稳定性、可靠性是不言而喻的，一个不稳定、不可靠的网络不但影响政务工作的顺利进行，还会影响政府在社会公众中的形象。因此在濮阳市行政审批和政务信息管理局政务外网设计和建设中，从各个方面充分考虑网络线路的质量和设备的冗余，考虑政务业务系统可能对外网的更多需求，在稳定性没有保证的情况下，考虑其可能的备份措施。

10.3.3.5 经济性原则

在网络系统设计和建设中，尽可能地充分利用和保留原有各种网络资源及计算机

系统资源等，保护已有投资，避免投资浪费，节约政府资金。网络结构和带宽可以满足当前及今后一段时期内政务外网上各种应用的需求。新增设备选用上充分考虑其兼容性、可扩展性及性能价格比。

10.3.3.6 可扩展性原则

在外网设计和建设中，在网络建成的基础上，在不影响外网上各种应用的前提下，根据业务的需要，网络、系统可以进行顺利扩展或者平滑升级。网络可扩展的关键在于能否实现合理的模块化设计，采取模块化的设计可以根据网络需求的变化，在不影响现有网络运行的状况下，迅速扩展。因此，整个外网工程中，在设计上要尽可能选用模块化的网络产品。

10.3.4 系统总体结构和逻辑结构

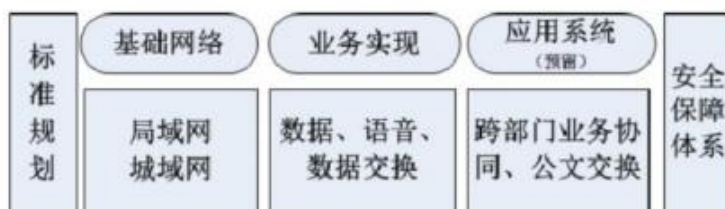
政务外网平台为树形结构，包括一级（国家）网络、二级（自治区级）网络、三级（市）网络和四级（县区）网络。每一级网络基本由广域骨干网、城域网、用户接入网等构成。

按照国家、自治区统一规划和标准规范，濮阳市行政审批和政务信息管理局电子政务外网将国家电子政务外网平台在濮阳市进行延伸，通过项目建设，为政务外网应用服务提供可靠、安全、高速、高效支持。

按照网络功能、管理层次和服务类型，总体结构可以分为：

1. 按照网络功能划分，总体结构可分为广域骨干网、城域网和接入网。广域骨干网由上连濮阳市节点的县节点组成，城域网是县本级横向网，接入网由县级各政务部门接入局域网组成。

按照逻辑层面划分，可分为基础网络层、业务实现层和应用系统层。



电子政务外网总体结构图

根据政务外网所承载的业务和系统服务类型，将政务外网划分为公用网络区(Global)、专用网络区(VPN)和互联网接入区(Internet)三个功能域，分别提供政

务外网互联互通业务、专用VPN 业务和互联网业务。



政务外网逻辑功能区域图

其中：

(1) 专用网络区：是依托外网基础设施，为有特定需求的部门或业务设置的 VPN (Virtual Private Network, 虚拟专用网络) 网络区域，VPN 网络区域主要为少数部门的特定业务数据传输提供安全通道。濮阳市电子政务外网采用MPLS VPN技术将有特定需求的业务数据与其他数据安全隔离，用于满足部门特殊需求。该区域采用私有地址，在骨干网上采取标签方式进行交换。

(2) 公用网络区：采用国家政务外网公共 IP 地址和地方公共IP 地址规划的网络区域，是政务外网的主干道，实现各市县、各部门互联互通，为跨地区、跨部门的业务提供认证、目录交换、公共应用服务等共性支撑平台。

(3) 互联网接入区：是政务部门通过逻辑隔离手段安全接入互联网的网络区域，满足各级政务部门利用互联网的需要。在互联网接入区，采取了综合的安全防护措施，对互联网接入业务提供安全防护。政务外网构建互联网安全接入平台，实现各政务部门办公的公务人员利用互联网通道，通过数字证书认证、密码技术和 VPN 技术，安全接入电子政务外网，访问指定的业务应用系统。

10.3.5 项目设计方案

10.3.5.1 标准规范建设内容

(1) 标准规范建设的原则

标准化规范是濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目建设的基本保障。在严格遵循国家电子政务外网和河南省电子政务外网有关规范标准的基础上，结合具体情况，逐步建设适用的信息化标准规范和保障体系。濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目标准规范建设遵循以下原则：

1. 因地制宜原则

要根据项目建设的具体实施情况和应用水平，在国家、自治区电子政务领域没有相应的标准、规范参考时，因地制宜地制定符合濮阳市行政审批和政务信息管理局电子政务外网建设实情的标准规范。

2. 统一兼容原则

系统要求开放性好、标准化程度高，系统建设应与现有的一些单位局域网系统平台兼容。在标准、规范制定中，国际上有标准的，要尽量参照国际标准；国家、自治区已出台建设标准、规范的，要遵循国家、自治区的标准。

3. 政令畅通原则

本项目制定的标准规范，对规范指导濮阳市行政审批和政务信息管理局电子政务外网项目建设具有重要意义，要维护濮阳市行政审批和政务信息管理局电子政务外网管理机构政令的畅通，切实执行。为避免本项目建设标准规范只制订不执行，或者执行效果不理想等情况，在出台相关的业务标准、技术标准、项目建设等标准规范时，必须要有相应的后续落实措施。

4. 安全可控原则

落实国家网络安全和信息技术安全有关政策，优先采用自主可控的产品及密码算法，增强网络安全可控能力；加快构建安全可信基础环境，推动标准落地实施，切实保障信息系统安全。

5. 可管理型原则

系统设备易于管理、维护，操作简单，便于配路，在安全性、数据流量、性能等方面能得到很好的监视和控制，可以进行远程管理和故障诊断。

(2) 标准规范框架

濮阳市行政审批和政务信息管理局电子政务外网项目标准规范分为总体标准、网络及通信标准、数据交换标准、信息安全标准和工程管理标准五个大类。标准规范框架如下图所示：



标准规范框架结构图

(3) 标准规范建设内容

1. 总体标准建设

总体标准包括本项目建设所需的总体性的标准与规范。从工程建设角度看，总体标准的建设内容是根据本项目建设总体方案，从框架性思路出发，制定本项目所涉及的基本术语、标准化指南、标准编写规则等方面的标准，以保证项目工程建设高效、健康和稳定发展，减少重复投资和互不兼容。

总体标准中重点建设的标准有以下三项：

a. 术语

术语是本项目建设过程中所使用以及形成的基本概念的语言指称。对这些概念进行正确的语言指代，并将其内涵定义和外延定义清晰描述出来，是本项目要解决的基本问题。

b. 标准化指南

标准化指南是根据本项目标准体系框架及其所涉及的标准化对象和内容，按照一定的主题和逻辑结构系统阐述所涉及的各标准的主要内容；是整个项目标准化建设的指南性文件。本项目标准化指南对推动和促进本项目在标准化、规范化的道路上健康发展，应具有极为重要的指导作用。

c. 标准编写规则

标准编写规则应给出标准的结构和编写标准的基本要求，规定标准要素的编写规则、标准条文的编写规则、标准的编写格式以及标准的出版格式，对于本项目的标准的编写、审查、出版和管理具有直接的指导作用。

2. 网络及通信标准建设

网络及通信标准分体系包括为本项目各应用系统提供基础通信平台的标准和进行系统设计时应遵循的网络标准。本项目网络及通信标准主要内容包括：网络工程建设规范、网间互联技术规范、网络IP地址分配规范、网络域名命名规范、电子邮件地址命名规范、通信设备命名规范、通信技术标准等。该分体系以采用相关国际标准、现有国家和自治区标准为主。

3. 应用支撑标准建设

应用支撑平台是基于可信消息管控的应用支撑架构，是承载业务系统协同工作的软硬件综合平台，能提供统一的接入认证与授权服务以及可信的应用传输与信息交换服务。

应用支撑标准分体系通过制定统一接入认证、可信应用传输以及系统间的接口规范，为本项目各应用系统提供安全服务和可信的应用环境，实现安全互联互通和安全信息共享。其主要内容是：应用支撑平台通用技术要求。该分体系以采用现有相关国际标准、国家标准和自治区标准为主。

4. 信息安全标准建设

为了避免网络系统、应用系统和数据资源遭受来自系统内外各类主动或被动的攻击，保障各级系统稳定、有效地运行，本项目必须建立完善的安全保障体系。主要内容包括：信息系统安全等级保护通用技术规范、信息系统安全管理规范、信息系统网络安全规范、数字认证体系安全管理规范、操作系统安全使用技术规范、访问控制管理规范等。该分体系以采用国家、自治区电子政务外网相关标准和国家信息安全相关标准规范为主。

5. 项目管理标准建设

本项目将按照科学的管理方法，利用标准化手段，对项目建设进行全方位、全过程的管理和监督。项目管理标准指本项目从立项、开发、监理、验收、运行、管理等环节应遵循的管理规范标准的集合。主要包括如下内容：项目管理规范、运行管理规范、安全管理制度、工程建设管理规范等。

10.3.5.2 信息资源规划

根据数据管理需求、应用特点及应用规划,建设全局性、基础性数据集成环境,实现数据统一、集中管理。

1. 数据类型

政务外网数据分为信息公开型、统计分析型、信息服务型三类。

(1) 信息公开型数据

是指各级政府部门在日常工作过程中生成的数据,此类数据由人工录入或从办公系统中产生,为信息公开发布平台提供数据支持,包括组织机构数据、政务公开数据、政府部门信息数据、标准代码数据、政策法规数据等。

(2) 统计分析型数据

是指通过对业务数据进行统计、汇总、分析加工后产生的数据,以及根据统计分析决策需要,建立主要数据的数据仓库,为领导决策支持系统提供数据支持。

(3) 信息服务型数据

指各类对公众提供政务服务的信息,为公众的在线办事和在线查询提供数据支持。

2. 信息资源规划

进行信息资源规划,必须考虑解决业务流程优化和功能建模、数据流分析、数据建模和数据标准化问题,实现信息共享、资源整合和业务协同。

信息资源规划主要工作内容为:

(1) 组织数据录入

对新建的数据库结构,需要在应用开发的开始阶段编制数据录入程序,将整批业务数据加载到新数据库中,或者在应用系统运行的过程中录入加载数据。

(2) 组织数据转换

对已积累的数据库资源,不论原先的结构如何设计,都是重要的信息资源,需要按基本表的结构标准编制数据转换加载程序。

(3) 重整数据结构

以信息资源规划设计方案中基本数据库和数据标准为标杆,来逐一衡量、评估已有数据存储的结构,找出具体的差距,确定哪些数据结构可以修改、补全,哪些数据结构不合理应该抛弃,还要增加哪些新的数据结构,从而形成高可利用的数据环境的数据结构。

10.3.5.3 应用支撑系统设计

应用支撑平台是整个系统建设的核心。该平台中包括了用户组织机构建模、资源权限管理、数据字典管理等一系列基础配置功能。借助于系统配置管理平台可以快速构建新的系统以及对旧的业务系统进行润色。应用支撑平台组件与功能设计内容主要有：

1. 统一用户身份管理

实现对组织机构、用户、角色、应用系统、权限及授权关系的集中管理，解决各个业务应用系统建设中存在的基础功能的重复建设和投入等问题，为实现数据整合、信息共享、流程优化提供基础保障。避免不同的业务应用系统之间多重身份、基础资料不唯一等情况。

2. 统一身份认证与单点登录

每个系统都需要用户信息、用户认证、权限管理、权限查询的功能模块，且功能特性基本相同，将他们的规律总结起来，开发一个公共系统可以提高各个系统的开发。实现用户一次登录、网内通用，避免多次登录到多个应用的情况发生。实现濮阳市行政审批和政务信息管理局电子政务外网工程中所有系统管理用户认证、授权信息的统一入口，即权限门户。支持到文件证书、UKEY 等安全认证方式。

3. 与 CA 认证集成

帐号验证数据源可以与 CA 认证中心进行集成绑定，外网用户登录时都可以使用 CA 证书进行登录，识别身份和权限。数字身份认证的作用在于实现对网络用户的身份鉴别、权限认证和责任认定，确保网络通信中用户(含设备)身份的真实性与合法性，用户访问与操作权限的确定性，用户操作行为与责任的可鉴别性与不可否认性。基于网络信任体系，实现了网络通信中可靠地识别一个用户的身份、行为和责任。

10.3.5.4 数据处理和存储系统设计

(1) 数据处理系统

数据处理系统的建设目标是构造一个功能齐全、运行高效、使用灵活、维护方便、易于扩展、投资省、安全可靠的主机平台，为业务系统提供可靠、高效的支撑平台。

(一) 数据处理系统建设原则

1. 高可用性

保证充分的处理能力，具有良好的性能以能够支持业务系统的运行；同时，考虑

到随着用户量的扩充，系统要求会有所提高，因此要能够既满足现有的需求，又能够有一定的前瞻性，充分考虑可出现的新业务，对系统留有足够的冗余。

2. 高可靠性

要能够提供连续服务，主机系统具备可靠性、安全性及故障恢复能力，保证系统能长时间不间断运行。

3. 可管理性和可维护性

为了保证系统安全可靠的运行，整个系统的管理和维护是十分重要的。整个系统的结构应该是简单的、易于管理和维护的。

4. 可扩展性

随着新业务需求的发展，主机系统的扩充能力也是系统设计需要充分考虑的因素。

5. 实用性

设计方案要充分考虑到实际需求和经济承受能力，量力而行。

(二) 主机系统需求分析

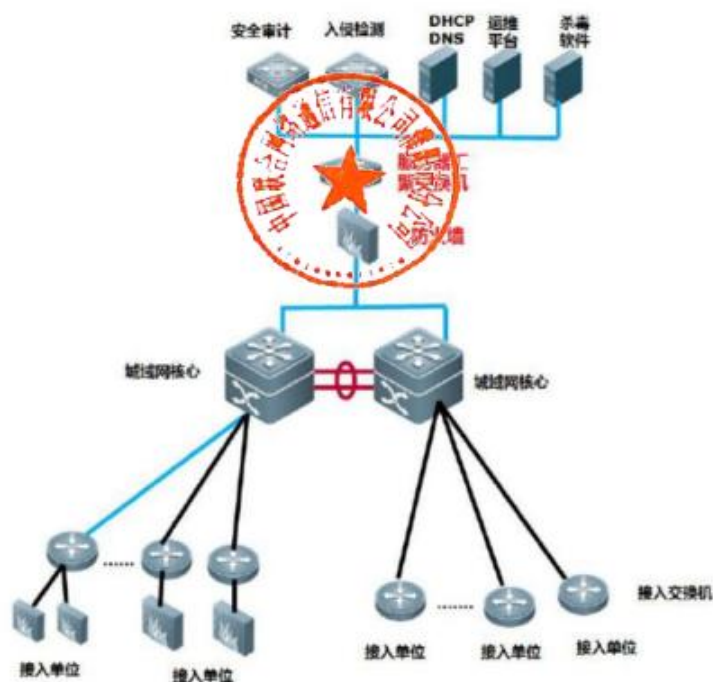
用于承载应用支撑平台的主机需要较高的 CPU 和内存处理能力以及一定的可靠性；用于承载数据库的主机仅用于运行数据库，数据库的容量以 GB 为单位增长，需要高性能的 CPU 处理能力，大容量内存为数据缓存服务，并需要很好的 IO 性能，数据库应用是对系统各方面性能要求最高的应用，可靠性要求也非常高；用于承载业务应用系统的主机需要一定的 CPU 和内存处理能力。

(三) 主机系统服务器性能

主机系统服务器性能从定性分析和定量分析两方面解读。主机系统服务器性能的定性分析包括以下几个方面：可靠性(Reliability)、可用性(Availability)、可扩展性(Scalability)、易用性(Usability)、可管理性(Manageability)，即服务器的RASUM 衡量标准。本项目根据自身应用环境选择 TPC 体系作为评测标准。

(2) 存储系统

存储系统为数据存储、数据交换、数据共享等业务提供安全、快速、可靠的数据支撑，并实现对迅速增长数据的高效管理。存储架构图如下所示：



10.3.5.5 网络系统设计

(1) 城域网结构

濮阳市行政审批和政务信息管理局电子政务外网是濮阳市电子政务外网的重要组成部分，横向城域网主要用于同城政务部门互联，是全市政务部门提供互联互通、信息共享的基础平台。

为保证网络可靠性，提高数据转发效率，降低网络复杂度，濮阳市行政审批和政务信息管理局电子政务外网城域网采用星型拓扑二层扁平化结构，即分为核心层和接入层两个层次。此外，政务外网与互联网之间为逻辑隔离，建设统一互联网出口。

1. 网络架构

(1) 城域网核心层由两台高性能、高可靠的核心交换机组成，负责本级城域网内数据的高速交换，并互联各个委办局。双核心交换机支持虚拟化，对设备进行双机冗余保护，当一台设备出现故障，重要的业务可手工切换至另一台设备。

(2) 两台核心设备之间通过万兆光纤实现trunk，核心层和接入层之间通过采购运

营商线路连接；机房内的网络设备、安全设备、服务器设备及管理设备之间通过千兆多模光纤连接。

(3) 统一互联网出口，互联网与电子政务外网安全逻辑隔离，为接入单位、乡镇(街道)提供互联网服务。为提高可靠性，互联网带宽采用运营商多条链路，实施冗余和负载分担。

2. 各区域设备部署

(1) 公用网络区：部署基础网络服务、业务监控运维服务器、杀毒软件服务器等，通过 MPLSVPN 技术与其他区域逻辑隔离，管理人员通过网络对位于该区域的本部门服务器进行信息更新和管理。部署入侵检测，安全审计，漏洞扫描，防火墙等安全系统，提供全网网络安全保障。

(2) 互联网接入区：提供统一的互联网出口，满足各部门访问互联网的需求，同时为移动办公提供互联网汇接。互联网出口采用不同运营商的两条链路，实施策略路由、流量控制、链路负载均衡策略；为保证安全，按照等保要求，部署防火墙、入侵防御系统。

(3) 专用网络区：依托政务外网基础设施，为有特定需求的部门或业务设置的虚拟专网区域，主要满足部门纵向业务的需要，实现不同部门、不同业务逻辑隔离。该区域采用私有地址，在骨干网上通过标签(MPLS VPN)进行数据传输。

(2) 政务部门接入方案

接入设备作为电子政务外网的终端网络的连接设备以及城域网网络的边界，负责将单位部门相关终端、主机、服务器接入电子政务外网。

对于各个通过专线方式接入政务外网的接入单位，网络内部私有地址复杂，为了保证各单位快速灵活地接入电子政务外网，城域网接入设备需要具有 MCE 及 NAT 的功能。同时，考虑到各单位的内部主机在访问政务外网时存在同一主机能够访问多个纵向 VPN 业务的情况（如同一台主机既能访问互联网 VPN，又可访问公共资源VPN），从简化技术、实现节省投资的角度，濮阳市行政审批和政务信息管理局外网接入最终采用简单接入模型。具体如下：



单位接入模型

该接入模型中，将接入单位和乡镇政府划归网络接入层，其中办公大楼采用千兆光口通过裸光纤链路连接，通过MSTP（带宽1000Mbps）链路，连接到城域网核心设备上。接入单位存在同时需要接入互联网区、公用网络区和专用网络区。

（3）城域网基础线路选择

城域网网络核心由两台高性能交换机设备组成，它们之间通过设备万兆口捆绑互联，提供互联带宽。核心交换机支持10G性能扩容。核心设备与服务器、安全防控设备之间通过多模光纤互联，提供链路带宽。

各相关单位采用光纤链路及 MSTP 链路的核心设备连接，可扩展性考虑，结合实际需求分析，通过专用光纤链路连接，通过100Mbps专线链路的使用权与核心设备连接，保障满足承载业务应用需要。

（4）互联网出口方案

做为整个电子政务外网对互联网的出口，政务外网互联网出口同时承担着两方面的作用：一是电子政务外网内所有用户访问互联网的出口；二是公众访问电子政务外网综合门户网站的通道。互联网出口建设方案应有如下考虑。

（一）设计原则

1. 高性能。电子政务外网内部所有用户对互联网的访问均需通过此出口，数据访问量大，人数众多，故此出口在建设过程中涉及的所有设备必需具备高性能指标，如路由转发性能，包交换能力等。

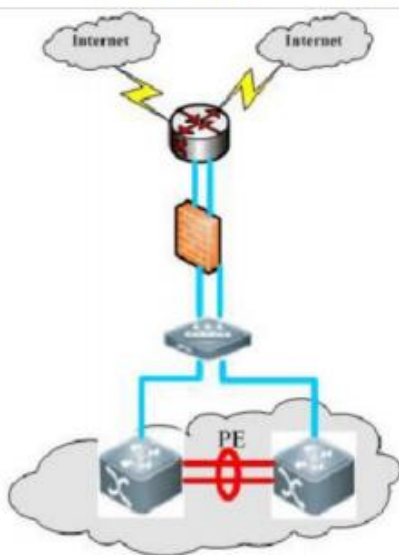
2. 高可靠。承担网络出口的所有网络设备必需具备高可靠性要求，以确保整个政务外网内部用户对互联网的正常访问。

3. 高安全。互联网出口是电子政务外网与互联网之间的纽带，它的安全性对电子政务外网的安全具有至关重要的影响。所有来自互联网上对电子政务外网的攻击和入侵等都应得到相应的控制。因此，构建互联网出口的网络设备具有强大的安全特性。

4. 可扩展。互联网出口建设必需考虑可扩展性。所有的网络设备应具有相应的扩展能力，同时组网结构应具有相应的发展能力，以便今后业务发展起来能够根据需要随时扩展互联网出口。

(二)出口线路方案

根据濮阳市行政审批和政务信息管理局政务外网互联网出口的实际情况，并考虑到未来的发展趋势，需要建立一个优化、稳定的电子政务互联网出口。



互联网出口拓扑图

1. 为了更好地实现网络出口的安全与稳定，采用两条互联网出口链路，实现线路冗余。

2. 在互联网出口具备双线路的情况下，必须提供高性能的策略路由和负载均衡，确保链路充分利用。考虑到应用、流量和用户增加以及互联网出口功能需求的增加，

采用防火墙设备实现高性能NAT(地址转换)。

10.3.5.6 IP 地址规划

(1) IP 地址规划原则

濮阳市行政审批和政务信息管理局、濮阳市电子政务外网线路租赁服务项目IP地址规划思路如下：

1. IP 地址规划将遵循有关规划和指导意见；
2. IP 地址规划主要涉及到网络资源利用的方便以及有效的管理网络的问题，合理的 IP 地址规划有利于网络的管理；
3. IP 地址的合理分配是保证网络顺利运行和网络资源有效利用的关键。本项目城域网 IP 地址的分配应该尽可能地利用濮阳市行政审批和政务信息管理局电子政务外的私有地址空间和公用网络区地址空间，充分考虑到地址空间的合理使用，保证实现最佳的网络地址分配及业务流量的均匀分布；
4. IP 地址的规划与划分应该考虑到网络的后续规模和业务上的发展，能够满足未来发展的需要；即要满足本期工程对 IP地址的需求，同时要适当考虑未来业务发展，预留相应的地址空间；
5. IP 地址的分配必须采用 VLSM (变长掩码)技术，保证 IP 地址的利用效率；
6. 采用 CIDR 技术，减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小；
7. IP 地址规划要和网络层次规划、路由协议规划、流量规划等结合起来考虑。IP 地址的规划应尽可能和网络层次相对应，自上而下规划；
8. 充分考虑了网络层次和路由协议的规划，通过聚合网络减少网络中路由的数目和地址维护的数量，也利于分级管理。

(2) IP 地址分配

按照上述 IP 地址规划思路，濮阳市行政审批和政务信息管理局电子政务外网 IP 地址分配如下：

1. 分配的正式IP地址段部分地址，用于公用网络区服务器的IP地址一对一映射和访问国家、公用网络区资源时的 NAT 地址池。
2. 分配的地址，用于用户局域网，根据接入单位规模，每个接入单位、乡镇可以分配1个 C 类(255 台主机)地址。
3. 设备管理 (Loopback) 地址

从分配到的正式地址段和私有地址段中选取，每台设备各取一个作为设备管理地址，子网掩码统一为 255.255.255.255。

4. 设备互联地址

濮阳市行政审批和政务信息管理局城域网设备互联地址，从分配到的私有地址段中选取，子网掩码统一。

5. 互联网出口地址

互联网出口 IP 地址(接口地址、NAT 地址池、服务器映射地址等)由我公司提供。

市级网络 IP 地址分配、管理和使用由市级网管中心负责，政务外网 IP 地址采用公有 IP 地址和私有地址两类地址混合使用，其中，政务外网公有IP地址主要应用于政务单位接入外网的转换地址、政务外网公用网络区服务器地址；政务外网私有IP地址主要应用于政务单位接入用户地址、内部服务器地址、网络设备互联和管理地址等。濮阳市行政审批和政务信息管理局城域网建设的地址规划，遵循濮阳市电子政务外网统一的 IP 地址分配规范，按照电子政务外网管理中心分配的地址规划城域网内地址，保证后期濮阳市行政审批和政务信息管理局城域网与电子政务外网的正常对接，杜绝发生政务外网上IP地址冲突问题，实现当地城域网之间的互联互通。

1. 专网网络 VPN

统一单位内部通过专用网络区市县纵向访问时（国家、自治区、市、区县），使用局域网内的私有 IP，不做 NAT 转换。县、乡单位局域网地址统一规划，避免冲突；如果单位内部局域网地址与规划不一致，甚至冲突时，在PE上发布服务器明细路由，同时在局域网中避开上级服务器的IP地址。

2. 公共网络 VPN

接入政务外网的单位访问公共网络区时，将统一分配的地址用于局域网出方向 NAT 源转换地址。使用单位如果需要向其他单位提供服务，则在单位接入设备上配置静态 NAT 映射，实现共享服务器地址对外映射。

3. 互联网访问 VPN

公共 IP 地址用于互联网访问出方向NAT 源地址转换和互联网访问区内政务外网服务器地址对外映射，不用于局域网终端地址分配。政务外网数据流在经过互联网出口时，在互联网出口的防火墙进行 NAT 转换。

10.3.5.7 路由、VPN 和域名系统设计

(1) 路由设计

路由协议的选择

路由协议的选择对网络的可靠性、灵活性、可扩展性有较大的影响。根据网络的结构，综合考虑管理和技术两个方面的因素，选择适合的路由协议。

路由协议的选择基本原则：

1. 管理上层次分明，局部的变动不影响上层路由配置和全局路由配置。
2. 技术上应尽量简单、灵活，以提高路由器的处理效率。
3. 能够反映出整个网络的层次结构，并与自治域、各结点子网的 IP 地址分配相结合，做到合理的路由聚合，减少路由表的长度，减轻路由更新给网络带来的负荷。

濮阳市行政审批和政务信息管理局电子政务外网网络平台选择的路由协议包括域间路由协议(EGP)和域内路由协议(IGP)。EGP 用于连接不同的自治系统，在不同的自治系统之间交换路由信息，主要使用路由策略和路由过滤等控制路由信息在自治域间的传播。IGP 即内部网关协议，在同一个自治系统内交换路由信息，其主要目的是发现和计算自治域内的路由信息。EGP 已采用 BGPv4 协议，用于与河南省电子政务外网广域骨干网，MP-BGP 用于政务外网广域骨干节点承载 VPN ipv4 路由。IGP 在城域网中主要承载网络设备间的互联路由，本项目 IGP 协议采用 OSPF 协议。

路由协议策略

1. 河南政务外网广域骨干节点已划分在area0域，濮阳市行政审批和政务信息管理局城域网节点划分在非0域，单位接入路由可根据实际情况选择动态路由或者静态路由。

2. 政务外网承载网路由由 IGP 即 OSPF 承载，包括互联地址路由、Loopback 地址路由、网管中心地址路由等；用户路由由BGP 或MP-BGP承载，包括用户业务地址路由、服务器地址路由等，以避免用户网络的业务路由震荡影响影响承载网路由。管理上亦可做到层次分明，局部变动不影响上层路由配置和全局路由配置。

3. BGP 的 AS 与自治区政务外网划分在同一 AS 中，利用自治区政务外网的 RR 和 BRR，交换 AS 内部的 BGP 全局路由，简化 BGP peer连接数量，提高网络路由的稳定性。

4. 由于电子政务外网用户业务是通过 MPLS VPN 来逻辑隔离，因此可根据实际需要将公共访问的业务网段路由引入到 IBGP 中，比如将 INTERNET 网关的缺省路由发布到IBGP 中。

5. 城域网接入网关启用 NAT 多实例功能, 依据访问区域的不同, 将来自不同业务的私有 IPv4 地址, 转换为公用网络区的国家公有 59 段 IPv4 地址, 或者部门 VPN 自行规划的私有 IPv4 地址。

承载网路由设计

承载网路由是指电子政务外网城域网广域网的网络设备所组成的互联路由。由于承载网设计在一个自治域系统 AS 内, 所以承载网路由设计演变为自治域系统内部网关协议的设计。根据路由协议的选择, 选用 OSPF 作为承载网的 IGP 协议。OSPF 可以在同一路由自治域中, 将网络分为若干个区域, 区域内的路由器共享区域内的网络拓扑结构信息, 区域间的路由信息通过区域边缘路由器进行传递。

1. 城域网内部互联端口划分为非 0 区域, 广域网骨干路由器划分为 0 区域。为避免路由环路, 不通过 OSPF 发布缺省路由。

2. 承载网设备均使用 Loopback 地址作为管理地址, OSPF 作为承载网的 IGP, 只负责承载互联接口网段和管理接口的地址传递, 实现 BGP、LDP 的邻居关系建立, 承载 BGP 会话、LDP 会话以及发布 CE 设备管理网段路由。OSPF 不引入直连和静态路由, 避免存在 OSPF type5 的外部 LSA 出现, 管理接口地址采用 network 发布。

3. 为加快 OSPF 邻接关系的形成, 如果一条链路上只有两台设备 启用 OSPF, 则将该链路两端的 OSPF 网络类型改为点对点模式, 即 point-to-point。

4. 为保证网络安全, 避免非法路由器或伪造的路由信息加入到网络中, 使全网路由出错, 导致网络瘫痪, 采用 OSPF 路由认证, 认证方式可以是明文或者 MD5。

5. 为实现纵向、横向数据流控制, 要对 OSPF cost 值进行全局规划。

用户路由设计

电子政务外网用户路由分成两部分: 一部分是全局路由, 另一部分是 VPN-IPv4 路由。全局路由由标准的 BGP 协议产生, 而 VPN-IPv4 路由由多协议 BGP (MP-BGP) 来承载。电子政务外网的 IGP 协议采用 OSPF, 其核心层、接入层节点划分在非 0 区域内。当构建 MPLS/VPN 拓扑时, 采取在 PE (核心层设备) 上运行 MP-iBGP 路由协议交换所有的 VPN 路由。

对于用户路由, 将连接用户业务网段的直连路由或静态全部引入到 IBGP 中: 来自不同 VPN 的用户私有 IPv4 地址, 通过单位接入 网关启用 NAT 多实例功能, 转换为公有 IPv4 地址后, 由 IBGP 发布 到全网。此外, 对需要公共访问的业务网段路由也引入到 IBGP 中, 比如将 INTERNET 网关的缺省路由发布到 IBGP 中。

(2) MPLS VPN 设计

濮阳市行政审批和政务信息管理局电子政务外网主要承载部委、区级垂直业务系统，以及本级后续部署的相关政务系统，部分系统将采用 VPN 承载。在电子政务二三级网络中，为了实现业务的隔离和安全，采用 BGP/MPLS IP VPN 进行安全隔离，根据业务类型和范围将 VPN 分为两类：纵向隔离 VPN、横向互通 VPN。

1. 部门纵向业务 VPN：承载市、县(区)各部门非涉密的纵向行业业务；

2. 横向互通 VPN：承载县本级单位、部门之间信息共享与交换的业务；

3. MPLS VPN 设计

纵向 VPN 上，承接国家、省、市电子政务外网平台的统一规划，下连各乡镇电子政务外网平台，在横向上能够方便连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等，负责部门各类业务在对应 VPN 的接入和本地业务和广域骨干网络的对接。

(3) DHCP 系统设计

DHCP 是 Dynamic Host Configuration Protocol 的缩写，它是 BOOTP 协议的扩展。DHCP 是一个局域网的网络协议，使用 UDP 协议工作，主要的用途是自动将 IP 地址传到请求地址的客户计算机，从而减少人工分配和跟踪分配客户机的 IP 地址所需的工作量。它分为两个部分：一个是服务器端，另一个是客户端。所有的 IP 网络设定参数都由 DHCP 服务器集中管理，并负责处理客户端的 DHCP 要求；而客户端则会使用从服务器分配下来的 IP 配置参数。

DHCP 工作原理：在一个使用 TCP/IP 协议的网络中，每一台计算机都必须至少有一个 IP 地址，才能与其他计算机连接通信。DHCP 是便于统一规划和管理网络中的 IP 地址，有利于濮阳市行政审批和政务信息管理局电子政务外网中的客户机 IP 地址进行有效管理，不需一个个手动指定 IP 地址。

(4) 域名系统设计

按照“国家政务外网域名规划与管理”要求及电子政务外网域名规划方案，濮阳市行政审批和政务信息管理局电子政务外网域名系统设计如下：

(一) 域名注册方式

域名以 4~5 段为主，原则上不超过 5 段。具体到某个单位，共有 3 种域名注册方式。

1. 纵向向系统上级机构申请注册。如农业局，可以向系统上级机构国家农业部申请类似的域名。

2. 横向向省级外网管理中心域申请注册。如农业局，可申请专用的域名。

3. 对于特殊的应用需求, 可以向国家外网管理中心申请四级域名。其中方式 1 和方式 3 需要在省级外网管理中心备案之后再向国家外网管理中心注册。

4. 也可向国家申请注册四级子域名。

(二) 命名原则

以 hnhcsdhx.cegn.cn 域名为例说明命名原则: (主机头/应用)。(县区简称+单位简称)。gxhcsdhx.cegn.cn, 其中, (主机头/应用)指 www、ftp、vod 等; (县区名简称) 单位简称规则, 单位中文简称首字母, 或单位中文简称首字全拼+后面字首字母, 或单位中文简称全拼, 也可采用英文简称。

(三) 域名服务规范

电子政务外网平台中的域名解析工作, 由各级域名服务器共同协作完成。这些服务器在进行规划和提供服务时, 必须遵循以下规范。

1. 逆向域名解析

电子政务外网中 IP 地址采用双轨制, 存在着公有地址和私有地址。对于私有地址, 不设置逆向域名解析。对于公有地址, 可以设置逆向域名解析, 该解析工作由 IP 地址段所属单位的域名服务器提供。

2. 正向解析工作方式

域名服务器的正向解析工作方式主要分为“轮询方式”和“递归方式”。电子政务外网中, 所有域名服务器都支持“轮询方式”, 例如对于域名

“www.hcsdhx.gx.cegn.cn”, 依次按照“.”、“cn.”、“cegn.cn.”、

“gx.cegn.cn.”、“hcsdhx.gx.cegn.cn.” 进行查询。电子政务外网中, 仅允许提供域名区域“gx.cegn.cn.”解析的服务器接受其他下级服务器的查询递归请求, 例如, 管理“nnsdpc.gx.cegn.cn.”区域的服务器, 可以将自己不知道的域名解析请求直接交付“gx.cegn.cn.”服务器进行解析, 而不需要执行“轮询”过程。

10.3.5.8 综合布线系统设计

本期工程将对濮阳市行政审批和政务信息管理局进行统一的综合布线改造, 部署超五类线综合布线系统构建千兆链路高速局域网, 使用大量高效、方便、安全的线缆连接, 以保证各个应用系统的顺利启用。

根据各个楼层对不同信号的接入需求, 本次工程大楼综合布线系统采用超五类非屏蔽布线产品。本次工程综合布线系统建设分为五个部分: 用户工作区建设、水平布

线子系统建设、配线间建设、垂直干线子系统建设、机房建设。

用户工作区建设：主要指信息点及其他接入点的建设。办公大楼地插式信息点配置2个网口，网络链路使用1个，1个备用；桌面式信息点配置1个网口，网络链路使用1个，所有网口均采用超五类线并放置至配线架配线架。

水平布线子系统建设：水平布线子系统由从各配线间到对应的用户工作区的线缆组成。本次工程采用超五类线布线，大楼布线接入交换机上行带宽为1GB。

配线间建设：根据办公楼实际使用情况，在各楼层设置配线间、综合柜架，根据信息点需求及实际使用情况配置楼层交换机、24口配线架和光纤配线模块。

垂直干线子系统建设：垂直干线子系统是数据传输的“大动脉”，是综合布线系统的关键部分。它由主机房内的主配线架至各配线间内配线架之间的楼内光缆组成。本次工程各楼层交换机通过楼内千兆链路联至县党政办公大楼的汇聚交换机，经汇聚后以千兆光纤链路接入新增的核心交换机，形成高速率的局域网。

机房建设：本次工程利用办公大楼电子政务外网管理中心机房作为核心机房，主机房用于部署城域网核心设备，公用网络区和互联网区的安全设备，以及部分大楼综合布线系统的网络设备。

10.3.6 项目实施人员

针对本次项目，我公司组织了专业的技术团队，以项目经理为主导，技术负责人带领技术人员展开项目的实施，文档管理人员及时记录实施过程中的数据，并做好项目资料建档管理。

10.3.6.1 领导和管理机构

1. 项目建设领导小组

本项目由濮阳市行政审批和政务信息管理局电子政务外网项目建设工作领导小组统一领导，负责项目建设与运行的领导工作。研究推进电子政务外网项目实施计划，协调解决电子政务外网项目在组织实施过程中的存在问题，监督检查项目实施工作。

2. 项目建设办公室

项目建设应在相关主管部门的统一领导下，成立“电子政务外网项目建设工作领导小组”（以下简称“领导小组”），统一组织、协调本项目的建设。在领导小组下设“电子政务外网项目建设办公室”（以下简称“外网项目办”），作项目建设的执行机构。



项目组织机构图

◆ 技术职责划分

项目经理：全权负责项目的实施、决定项目的工作计划和决策。

技术负责人：保证项目设计及实施的准确性和可靠性，对项目的需求分析、设计、关键问题的解决、风险的规避及新业务的开发提供思路、指导和咨询。

技术工程师：对本项目涉及的所有软硬件系统提供专业性维保服务。

◆ 技术人员考核

A 公司将对工程师进行定期考核，每半年一次，考核指标有任务完成及时性、任务完成正确性、月度工作总结、周工作总结等。在考核期内达不到要求的将进行为期一个月的下岗培训，培训后仍达不到要求的将予以辞退。

B 技术工程师在接到技术服务请求后，按公司规定做出合理的服务方式及时为用户排除故障，因特殊情况不能及时解决的应报主管领导出示处理意见。

C 技术工程师到达用户所在地时应出示工作证件，工作中不得向用户索要食物、香烟等物品，进入用户机房前必须按其要求穿戴鞋套。

D 技术工程师返回公司后，及时向领导汇报有关情况。《故障处理报告》是对工程师工作情况的证明，同时作为公司了解工程师工作情况和对他们年终考核的依据，在工程师处理好用户反映的问题之后，务必填写此报告，并由用户代表签字生效，一式两份。

E 技术工程师应认真热情为用户服务，做到有问必答，有求必应，不得因任何原因与用户发生争执，遇到特殊情况需及时电话与主管领导联系，请示处理意见。

针对发生的信息系统安全事件，为了便于警方查案，保留证据，同时保障信息系统安全运行，减少对正常业务造成的影响，本项目在运行中需加强对安全案件处置的管理，制定相应的安全处置预案，提高对信息安全案件的处置能力。

4. 加强培训机制，建立人才队伍。

加强运维管理人员的技术和管理策略培训，通过标准化的流程和相关制度约束，保证网管策略自上向下地有效贯彻。加大人才培养力度，建立激励长效机制，培养懂技术、懂管理、精通业务的专业人才。

5. 建立考核评价体系。

建立有效的考核评价体系，明确运行指标，实现量化管理，并配套行政手段，督促管理措施的落实。

6. 管理制度化、规范化。

网络运维管理过程中各参与要素的行为准则和工作程序制度化、规范化，提供高质量网络服务。

10.3.7 部署方案

10.3.7.1 到货验收

1、按照合同要求，在指定的时间内，将电子政务外网接入指定的单位。

2、外观检查

设备到货后，由业主及项目经理对设备外包装箱进行检查，根据项目要求，按照与业主约定的设备到货验收标准进行外观检查，如外包装箱是否破损，是否开箱，是否为原包装等。

3、开箱验收

业主、项目经理在现场对设备开箱，并进行装箱单检查，由业主、项目经理共同核对装箱单，检查箱内配件是否与装箱单相符。

4、设备上架

开箱验收完成，经业主允许在指定的位置由项目组人员对设备进行上架安装。

5、加电验收

基础环境准备就绪，在业主的许可下对设备加电测试，设备加电测试完成，打印设备信息，形成报告，出具设备加电验收单。

6、到货验收完成

开箱验收、加电验收无误后出具到货验收单。

10.3.6.2 项目实施机构

1. 具体实施机构

项目建设办公室是本项目的实施机构，负责项目的具体实施、管理和维护。项目管理办公室由项目综合组、工程组、财务管理组、安全组、运维组五个工作小组组成，人员主要由有关部门的人员组成。各工作组在项目建设的各个阶段明确职责、分工合作。

2. 专家咨询机构

为保证项目建设的科学性，在项目建设过程中，将聘请信息化领域专家成立专家咨询委员会，为项目的设计与实施提供咨询；审议工程总体设计方案，对重大技术问题进行论证，参与工程项目的检查、评估和验收等。

10.3.6.3 运行维护机构

濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网由濮阳市行政审批和政务信息管理局负责管理、运行及维护。

10.3.6.4 运行维护管理措施

濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网网络运维管理遵循集中监控、集中管理原则。濮阳市行政审批和政务信息管理局外网管理机构负责运维管理本项目建设的城域网，确保网络和各级政务外网应用稳定运行，防止发生对广域骨干网的攻击事件，保障濮阳市电子政务外网广域网安全。

在濮阳市市直电子政务外网建设和管理协调小组的领导下，主要做好以下几项工作：

1. 建立沟通机制。

濮阳市行政审批和政务信息管理局政务外网管理机构和各市直政务部门接入单位之间设立沟通渠道，建立定期和不定期的故障排除沟通机制，建立良好的问题排查机制，明确故障排查顺序，在制度上保证网间通信故障的准确定位和及时排查。

2. 制定事件处置预案。

制定科学合理的安全事件处理预案，明确安全事件处理流程，降低故障恢复时间，保障网络通畅和日常工作正常进行。

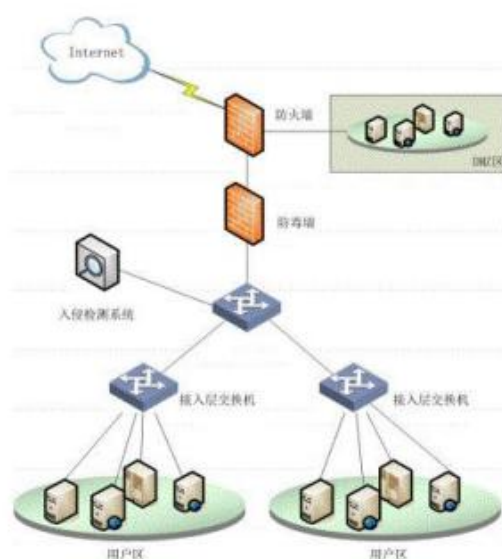
3. 制定安全案件处置预案。

10.3.7.2 网络系统建设方案

10.3.7.2.1 建设背景

随着我国信息化建设的深入，特别是电子政务的发展，以及第三方信息服务商的成熟和服务不断完善，计算机技术的应用发展而生根本性的变化，各级政府领导和机关工作人员信息化意识大大增强，办公业务领域的计算机应用不断普及，公文、信息处理的效率进一步提高；一支既懂办公自动化技术又熟悉机关业务的专业队伍已经形成。这些新成果充分说明，办公自动化工作已经具备了向更高层次进一步加快发展的必要条件。所有这些都为推进政府信息化建设奠定了良好而扎实的基础。

10.3.7.2.2 政务外网拓扑图



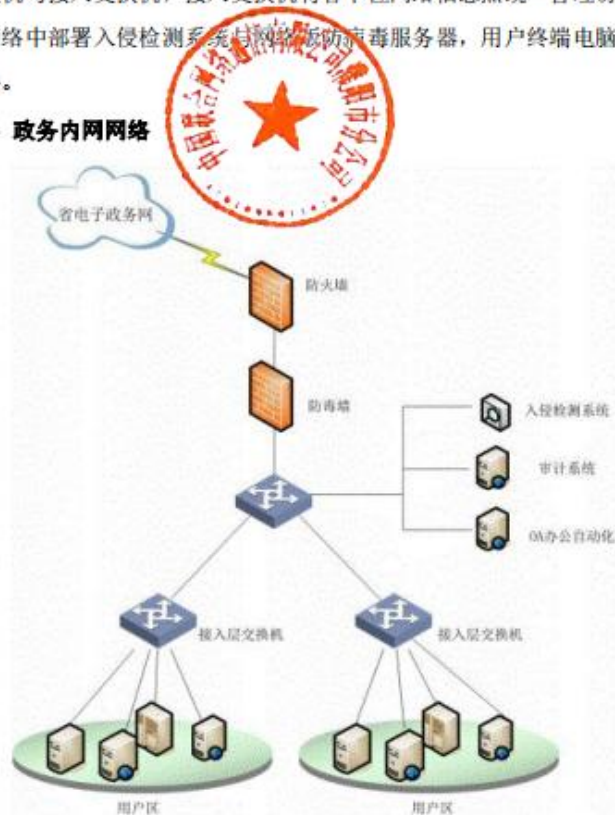
网络拓扑图

政务外网的网络架构采取扁平式架构，避免过多接点导致的网络故障。采用一台核心层交换机与两台接入层交换机，构成该网络系统的基础通讯平台。边界网络采用防火墙，入侵检测，防病毒网关等安全设备，为政务外网系统保驾护航，为的应用提供足够的安全性，可靠性。

政务外网专线光纤入户，接入弱电机房，与机房内的防火墙设备直接连接，核心交换机通过跳线与机房内接入层交换机连接。政务外网的设备安装在机房外网机柜内。

如上图所示，通过防火墙与互联网连接，防火墙负责网络边界安全与访问控制。下联一台核心交换机与接入交换机，接入交换机将各单位网络信息点统一管理访问政务外网。并且在网络中部署入侵检测系统与网络版防病毒服务器，用户终端电脑安装网络版防病毒软件。

10.3.7.2.3 政务内网网络



如上图所示，通过防火墙与省电子政务内网连接，入侵检测、安全审计等安全设备接入网络中负责安全防护。一台核心交换机与二台接入层交换机负责承载用户网络访问服务。防病毒服务器作为防病毒与安全审计系统的控制中心平台办公自动化系统服务器在网络中作为承载办公自动化系统的平台。用户终端电脑安装网络版防病毒软件。

业务访问方面，在防火墙上设置访问策略，与电子政务内网有信息交互的用户可以访问电子政务内网，而其它用户则不允许访问电子政务内网。入侵检测系统能够帮助网络系统快速发现攻击的发生，它扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的健壮性。

使用审计系统对用户的网络行为监控、网络传输内容审计（如是否在工作时间上

网冲浪、聊天，是否访问不健康网站，是否通过网络泄漏了单位的机密信息，是否通过网络传播了反动言论等），掌握网络使用情况，提高工作效率，网络传输信息的实时采集、海量存储、统计分析，网络行为信息验证，对网业络潜在威胁者予以威慑。

10.3.7.2.4 施工要求

1. 水平子系统

水平子系统的走线管道由两部分构成：一部分是每层楼内放置平传输介质的总线槽，另一部分是将传输介质引向各房间信息接口的分线管或线槽。从总线槽到分线槽或线管需要有过渡连接。

线槽中放置的双绞线应不超过线槽总容量的70%。在线槽中放置的双绞线密度过大会影响底层双绞线的传输性能。

水平线槽一般有多处转弯，在转弯处应留有足够大的空间以保证双绞线有充分的弯曲半径。根据 EIA /TIA569标准，五类4对非屏蔽双绞线的弯曲半径应不小于线径的8倍。最新的标准认为，弯曲半径大于线径的4倍已可以满足传输要求了。但有一点是重要的，即保持足够大的弯曲半径可以保证系统的传输性能。在水平线槽的转弯处，应有垫衬以减小拉线时的摩擦力。水平子系统线槽采用镀锌铁槽。

2. 垂直子系统

垂直子系统的线槽引向管理子系统布线柜的部分可能需要沿水平方向安装，由垂直向水平过渡应留有足够大的空间以保证电缆有充分的弯曲半径。

3. 管理区子系统

管理区子系统是工程施工中考虑最复杂的部分。这部分施工应充分考虑环境影响和端接工艺的影响。

电磁辐射是考虑管理区子系统安装环境的主要因素。电磁辐射的影响主要来自两个方面，一是环境对系统传输的影响，一是系统在信息传输过程中对辅境设备的影响。在建筑物内，环境对系统传输的影响主要来自强电磁辐射源，如电台，建筑物内的电梯，马达，UPS 电源，等。如果环境中这些干扰源的影响较大，因考虑采取屏蔽措施，或选择距离较远的位置。

布线系统的端接工艺是直接影响系统性能的重要因素。在 AMP 的系统性能参考手册中强调这部分工作应该由专业工程师安装。

连接配件的安装工艺主要影响布线系统的近端串扰和衰减，而这两个参数是判断系统性能的重要依据。在 AMP 的安装指南中要求双绞线的绞合拆开小于0.5英寸。

在管理区子系统还要考虑环境的通风，照明，酸碱度，湿度等条件，这些因素将

对端接配件造成腐蚀和老化，日久之后会影响系统的性能。

管理区子系统内的安全性也要加以考虑，端接配件最好安装在布线机柜或墙柜内。

4. 工作区子系统

工作区子系统在施工时要考虑的因素较多，不同的房间环境要求不同的信息墙座与其配合。在施工设计时应尽可能考虑用户对室内布局的需要，同时又要考虑从信息墙座连接应用设备（如计算机，电话等）方便和安全。

10.3.7.3 安全系统建设方案

本系统汇聚了大量电子政务的业务数据，数据的安全性尤为重要。目前在安全层面的考虑，较多的集中在传统的网络安全层面，对于数据生命周期中的入库存储、交换共享、调用跟踪、灾备保障以及数据分析的价值发挥等较为薄弱，而这些都将制约大数据中心的业务发展。总体而言，目前存在瓶颈和风险点，要通过本项目进行完善和解决。

信息安全是政务信息化建设不可缺的支撑平台，没有信息安全的坚实保障，电子政务就无法推进与前行。信息安全的要求将贯穿于整个信息化建设项目，因此，需要构建统一标准、统一规范、功能全面的安全保障系统，为大化瑶族自治县政务外网信息化业务提供切实可靠的信息安全保障，解决满足政务实际要求的安全保密性、信任和授权，以及安全监管等安全保障服务。

我方对政务外网网络安全负责，所建设政务外网符合三级等保要求，并通过国家三级等保认证，证书详见7.13章节。若我方中标，必会采取必要的技术和管理措施，确保政务外网安全。

10.3.7.3.1 风险分析

信息系统的安全是围绕信息系统的组成及其所实现的功能，对信息系统的运行及其所存储、传输和处理的信息进行安全保护所采取的措施。根据建设项目的组成与功能，分析其所面临的威胁，按照物理层、网络层、系统层、应用层和管理层面对其系统进行安全防护。

1. 威胁分析

政务外网与互联网逻辑隔离。网络使用者既有通过 Internet 进入访问的合法用户，也有来自内部及接入单位的工作人员，因此网络面临着两个方面的安全威胁：

(1) 外部威胁

1) 黑客扫描和入侵来自 Internet 的恶意入侵者可能通过发起恶意扫描和远程溢出等攻击, 渗透或绕过防火墙, 进入政务外网, 获取、篡改甚至破坏数据, 乃至破坏整个网络的正常运行。

2) 拒绝服务攻击

网站作为一个重要的信息发布、查询、对社会工作服务载体, 很容易受到恶意的流量拒绝服务攻击, 造成网站瘫痪, 无法提供服务。

3) 病毒或蠕虫侵袭

Internet 网络蠕虫病毒可能穿透防火墙, 渗透内部网络, 传播病毒。一旦遭受了病毒和蠕虫的侵袭, 不仅会造成网络和系统处理性能的下降, 同时也会对核心数据造成严重威胁, 导致业务应用中断。

(2) 内部威胁

1) 无意识的外部风险引入

由于安全技能和安全意识存在差异, 工作人员可能无意识将 Internet 上危险的、恶意的木马程序、恶意代码、蠕虫、网络病毒下载到内部网络, 这将给内部网络安全带来严重威胁。

2) 网络资源滥用导致新风险

因为各种 IM 即时通讯软件、网络在线游戏、P2P 下载软件、在线视频导致网络资源滥用, 网络性能下降, 数据传输拥塞, 严重影响正常工作, 形成新的威胁。

内部故意破坏需要考虑内部及各个接入单位中存在恶意破坏信息网络、系统和数据的可能。

2. 脆弱性分析

从系统和应用出发, 网络的自身脆弱性可以划分如下几个方面。

(1) 物理层脆弱性

物理层次的漏洞通常会被物理临近攻击所威胁, 包括未受保护的机房, 主机设备, 未进行电磁屏蔽的线路, 无线线路等。

(2) 网络层脆弱性

1) 数据传输

由于现在很多网络协议基于明文传输, 客观上存在被窃听和篡改的可能, 任何一个对通信进行监测的人都可以对通信数据进行截取。

2) 重要数据被破坏

目前尚无安全的数据库及个人终端安全保护措施，还不能抵御来自网络上的各种对数据库及个人终端的攻击。存储数据对于该应急系统来说极为重要，如果由于通信线路的质量原因或者人为的恶意篡改，都将导致难以想象的后果。

3) 网络边界

对网络中任意节点来说，其他所有网节点都是不可信任域，都可能对该系统造成一定的安全威胁。

4) 网络设备

网络中使用的网络设备，其自身安全性也会直接关系到信息系统和各种网络应用的正常运转。

(3) 系统层脆弱性

由于任何产品都不可避免的存在本地溢出，竞争条件，远程溢出等脆弱性问题，因此系统本身的脆弱性是不可能完全避免的。

(4) 应用层脆弱性

网站是对外宣传、开展业务的重要基地。但 Web 服务器被发现的安全漏洞越来越多，网站面临的安全问题不容忽视。

(5) 管理层脆弱性

安全的本质是管理，七分管理三分技术。在管理技术、组织结构、人员管理、制度建设等方面必须全方位加强建设，杜绝信息孤岛、人为破坏。

10.3.7.3.2 设计原则

信息安全系统建设应遵循统筹规划，同步建设，安全可靠，经济实用，灵活方便，技术成熟，统一标准，统一规范的原则进行。

1. 统筹规划，同步建设

做好统筹规划工作，制订总体方案。新建、改建、扩建网络平台及相应的业务系统，应当同步建设信息安全设施，保证信息安全与信息化建设相适应。

2. 安全可靠，经济实用

信息安全系统建设必须能够真正保护整个系统，保证网络资源受控、合法、安全地使用。信息安全系统在基本不影响系统功能和效率的前提下，须做到稳定、可靠地不间断运行。信息安全系统的设计要在安全需求、安全风险和安全成本之间进行科学的平衡、比较和折中，使整个信息安全系统安全、经济、适用，性能价格比合理。

3. 灵活方便，技术成熟

信息安全系统必须好用，并易于操作。同时要求信息安全系统允许增加新的安全组件与安全功能，保证系统安全性不断增长的需要。技术与产品选型时以技术成熟为优先考虑的原则。

4. 统一标准，统一规范

信息安全系统建设的各个部分都必须符合国家和关于信息安全的法律、法规。

10.3.7.3.3 安全系统建设内容

1. 物理环境安全建设

物理环境安全目的是保护网络中计算机网络通信有良好的电磁兼容工作环境，并防止非法用户进入计算机控制室和各种偷窃、破坏活动的发生。

物理安全主要涉及环境安全(防火、防水、防雷击等)、设备和介质的防盗防破坏等方面。具体包括：机房选址、物理访问控制、防盗窃和防破坏、防雷、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等。

2. 网络安全防护建设

本期濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目，为增强网络系统的可靠性和安全性，在公用网络区及互联网接入区均部署防火墙、入侵防御、入侵检测等安全设备。防火墙可视为一种 IP 封包过滤器，只有符合安全策略的数据流才能通过防火墙，起到安全隔离、访问控制的作用，具有非常强的抗攻击免疫力；IPS 设备对流经该关键路径上的网络数据流进行 2~7 层的深度实时分析，能精确的识别并自动拦截异常报文与异常流量；IDS 通过采取实时报警、事件登录，或执行用户自定义的安全策略，实现动态的安全维护。网络安全防护系统的建设能满足濮阳市行政审批和政务信息管理局电子政务外网安全等级保护三级要求。

3. 业务应用安全建设

主要指应用层的安全，包括程序安全、数据安全等。程序安全建设在应用软件开发的各个阶段，包括需求分析、设计、开发、维护及最后的文档编写等应遵循国标《信息技术 软件安全保障规范》(GB/T 30998-2014) 的要求。

数据的安全性将从以下两个方面进行考虑：

(1) 数据访问安全

根据不同内容的数据，以及不同级别的用户设置不同的数据访问权限。特定的数据（例如经费批准计划，经费使用记录等）只允许经过特别授权的用户进行访问，其他系统的数据根据角色不同设置授权。

(2) 数据传输安全

濮阳市行政审批和政务信息管理局电子政务外网的建设,外网线路传输达到国家建设安全标准。在远程进行数据访问和流程报批的过程中,通过数据压缩传输,加密传输等方法 and 措施,保证远程数据传输安全。

4. 信任体系建设

本项目利用已建成的国家电子政务外网数字证书建设信任体系。政务 CA 指国家电子政务外网电子认证全国服务体系,是依托政务外网,在全国范围内为党委、人大、政府、政协、法院和检察院以及各级政府部门提供信任服务,为运行在政务外网上的业务系统和用户提供技术标准一致、格式统一的数字证书,确保一张证书全网畅通,为不同单位开发的不同系统平台的互联互通奠定基础。证书服务采用集中受理、属地服务的模式,迅速、经济的为政务部门提供证书服务。

电子政务 CA 认证服务中心的建设是为了保证电子政务的应用安全,它的最终目标是在保证政务网络、应用安全的基础上,实现跨部门、跨地区信息资源共享、业务应用的互联互通。由外网信任源点作为根结点向注册中心统一签发数字证书,注册中心作为本地的根结点向本区域内分中心统一签发证书。

外网信任源点作为统一的根 CA,由统一的机构实行对二级 CA 结点进行监督管理并签发二级证书。数字证书是为实现双方通信安全提供电子身份认证。在利用互联网、政务外网或局域网时,使用数字证书实现身份识别和电子信息加密。数字证书中含有密钥对所有者的信息识别,通过验证识别信息的真伪实现对证书持有者身份的认证。

随着系统运行,业务系统业务数据逐步增加,为保障系统数据的安全,构建统一的用户 CA 认证体系,并给系统用户发统一的数字认证证书,用户需使用数字证书的方式实现高强度的身份鉴别,且利用key 存储用户的私钥以及数字证书,保证用户认证的安全性。数字证书可以实现以下功能:身份认证与授权:在信息的交换过程中,用于对双方进行认证,以保证交换双方身份的正确性;通信保密性:用于保证需保密的信息通过网络传输过程中不被窃取;访问控制:针对应用系统,确保只有授权的访问用户方可使用应用系统。

5. 建立健全信息化管理体制

建立分工明确、责任清晰、内容完善的信息化管理体制,强化信息化建设工作的统一管理和宏观把控,进行濮阳市行政审批和政务信息管理局电子政务信息化顶层设计。加紧完善信息化管理体系,强化统筹协调职能,明确信息化工作的主管处室和实施机构。促进电子政务外网建设工作,满足电子政务外网管理推进政务服务政务公开政府信息公开向基层延伸工作的要求。

10.3.7.3.4 安全域划分

1. 安全域划分原则

(1) 业务保障原则：安全域划分的根本目标是能够更好的保障网络上承载的业务。在保证安全的同时，还要保障业务的正常运行和运行效率。

(2) 保障性能和有效隔离原则：安全域划分应以不影响或损害业务信息系统的业务功能、性能为首先原则，在保证业务的性能的基础上对系统进行安全域划分、进行有效地隔离和安全防护。

(3) 简洁规范原则：安全域划分的简洁把握三个方面：一个安全域功能和边界通信的简洁，二是安全域之间关系(相连互通或隔离)的简洁，三是系统安全域整体结构的简洁。这就要求安全域不可分的太细，也不可分的太粗，要适度，要保持整体上的简洁。

(4) 等级保护原则：安全域的划分要做到每个安全域的信息资产价值相近，具有相同或相近的安全等级、安全环境、安全策略等。对于不同等级安全域的保护，从业务数据流角度来看，要求高等级安全域允许向低等级安全域发起业务访问的请求，保证发送数据的安全性，鉴别低等级安全域的合法性，对接受的数据进行完整性校验，对业务操作进行日志记录与审计；低等级安全域向高等级安全域只允许受限访问，保证发送数据的完整性，对业务操作进行日志记录与审计。

(5) 最小授权原则：安全子域间的防护需要按照安全最小授权原则，依据“缺省拒绝”的方式制定防护策略。防护策略在身份鉴别的基础上，只授权开放必要的访问权限，并保证数据安全的完整性、机密性、可用性。

(6) 立体协防原则：安全域的主要对象是网络，但是围绕安全域的防护需要考虑在各个层次上立体防守，包括在物理链路、网络、主机系统、应用等层次；同时，在部署安全域防护体系的时候，要综合运用身份鉴别、访问控制、检测审计、链路冗余、内容检测等各种安全功能实现协防。

(7) 与组织管理架构相适应的原则：安全域的划分应与信息系统的管理组织架构相适应，原则上由一个机构管理的信息系统部分应为一个或几个安全域。

(8) 与系统发展相适应的原则：安全域的划分应考虑到业务未来发展需要，在保持系统安全域模型相对稳定的前提下，能够顺利地进行调整、扩展和提升。

2. 安全域划分结

根据安全域划分原则，根据安全策略执行的需要，该项目电子政务外网可划分为网络骨干域、网络安全接入区、县级网络局域网三大类安全域，其中各大类安全域根据业务及应用特点又可继续进行安全域划分。

(1) 网络骨干域

网络骨干域指城域网核心层。

(2) 网络安全接入区域

网络安全接入区域指各县级政务部门局域网接入濮阳市行政审批和政务信息管理局政务外网的区域。

(3) 县级网络局域网

县级网络局域网指濮阳市行政审批和政务信息管理局政务外网网络管理中心区域，可以进一步划分为互联网出口区、互联网服务区、公用网络区及网管区。

10.3.7.3.5 信息系统安全等级

从信息安全管理角度来看，一般将计算机信息系统分为非涉密计算机信息系统和涉密计算机信息系统两类。其中，非涉密计算机信息系统是指不涉及国家秘密的计算机信息系统，包括党政机关用于处理对外职能事务或用于政府上网工程的信息系统；企事业单位不涉及国家秘密的信息系统；电信、科研、教育等部门向全社会提供的联接因特网的公众信息系统等。本项目信息系统基本上属于工作秘密即非涉密计算机信息系统范畴。因此，针对濮阳市行政审批和政务信息管理局应用系统，主要按照《GB/T 22240-2008 信息安全技术信息系统安全等级保护定级指南》的要求进行定级，并且依据《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》进行安全建设。

1. 等级划分思路

信息系统安全包括业务信息安全和系统服务安全，由于与之相关的受侵害客体和对客体的侵害程度可能不同，因此信息系统定级也应由业务信息安全和系统服务安全两方面确定。

(一)从业务信息安全角度反映的信息系统安全保护等级，称为业务信息安全保护等级。

(二)从系统服务安全角度反映的信息系统安全保护等级，称为系统服务安全保护等级。

确定信息系统安全保护等级的一般流程如下：

(1) 确定作为定级对象的信息系统。

(2) 确定业务信息安全受到破坏时所侵害的客体。

(3) 根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度。

针对对客体不同危害后果的三种危害程度描述如下：

一般损害：工作职能受到轻微影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

(4) 依据业务信息安全保护等级矩阵表，得到业务信息安全保护等级。

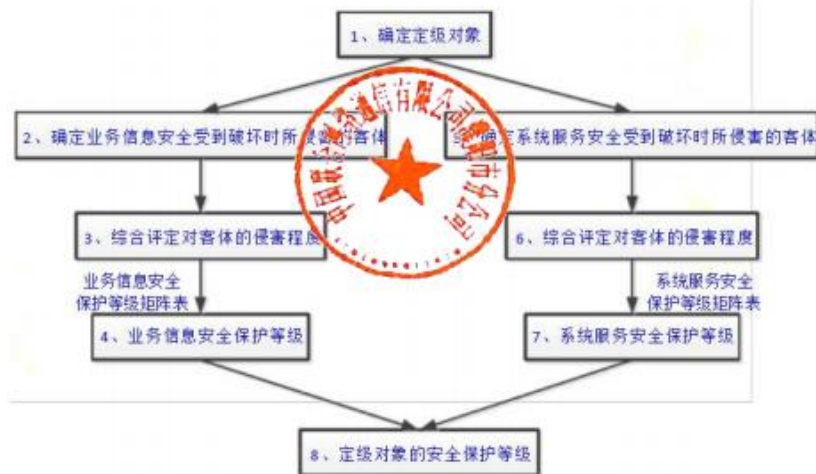
(5) 确定系统服务安全受到破坏时所侵害的客体。

(6) 根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度。

(7) 依据系统服务安全保护等级矩阵表，得到系统服务安全保护等级。（针对对客体不同危害后果的三种危害程度描述同第(3)点）

(8) 将业务信息安全保护等级和系统服务安全保护等级的较高者确定为定级对象的安全保护等级。

按照上述步骤确定信息系统安全等级的一般流程如下图所示：



信息系统安全保护等级确定流程图

2. 等级划分规则

(一) 业务信息安全保护等级的确定

1、业务信息描述

电子政务外网城域网采用星型拓扑二层扁平化结构，即分为核心层和接入层两个层次。城域网的核心层部署两台核心交换机，接入层部署路由器、接入交换机等。在安全设备部署方面，公用网络区部署入侵检测、安全审计、防火墙等，互联网接入区实施策略路由、流量控制、链路负载均衡策略，部署防火墙、入侵防御系统，满足电子政务外网安全建设要求。

2、业务信息受到破坏时所侵害客体的确定

濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目为各办公人员提供一个办公的统一平台，所侵害的客体是主要是公民、法人、集体和其他组织的合法权益，同时也侵害社会秩序和公共利益但不损害国家安全。客观方面表现的侵害结果为：(1) 影响各政务部门网上办公业务的开展，导致业务能力下降，造成不良影响等；(2) 不当的信息指引、错误的决策支持都会造成不良影响，引起公共利益的损害等。一旦遭到破坏后，对社会秩序、公共利益、领导决策等主要业务职能造成损害。

3、信息受到破坏后对侵害客体的侵害程度的确定

电子政务外网一旦遭到破坏后，将导致各政务部门的日常办公以及业务处理受到影响，容易造成业务系统数据的丢失，将对社会秩序和公共利益造成损害，使各政务部门的工作职能受到一定影响，业务能力下降，属一般损害。

(二)系统服务安全保护等级的确定

1、系统服务描述

电子政务外网属于为单位业务的顺利开展提供服务的网络平台，其服务范围及对象主要是各政务部门，主要服务内容是横向接入县本级和乡镇单位、纵向连接国家、自治区、县级、乡镇、规范各政务部门网络接入，建设统一互联网络出口，为各政务部门提供互联网访问服务。

2、系统服务受到破坏时所侵害客体的确定

系统服务受到破坏后，所侵害的客体主要是公民、法人、集体 和其他组织的合法权益，同时也侵害社会秩序和公共利益。侵害的 客观方面表现为：(1)对系统用户的合法权益造成侵害，影响网上办公业务的开展；(2)业务能力下降，造成不良影响，引起公共利益的损害等。根据《定级指南》的要求，出现上述两个侵害客体时，优先考虑社会秩序和公共利益，另外一个酌情考虑。

3、系统服务受到破坏后对侵害客体的侵害程度的确定系统服务受到破坏后，会对社会秩序和公共利益造成损害，使得用户单位的工作职能受到一定的影响，业务能力下降，部分影响主要业务职能开展、领导决策等，属一般损害。

10.3.7.3.6 安全防护系统

为使系统达到等保要求，网络安全区域划分边界，受控访问。边界互访综合采用多种成熟的安全技术，多层面面对信息网络系统保障。系统分别从网络、业务、物理、主机等方面考虑建设具体的安全防护措施。

(一)网络方面

1. 互联网出口

(1) 结构安全

互联网出口边界部署高性能、关键业务处理设备，出口链路采用不同运营商两条线路，不仅满足承载业务和数据传输需要，也具有负载均衡作用。

(2) 网络保护和恢复

出口边界的上联和下联线路具有倒换和冗余机制，其相应技术指标满足网络和业务需要。

(3) 访问控制

在互联网出口与城域网的网络边界之间部署入侵防御检测访问控制设备，启用访问控制功能。根据政务外网的承载能力，对网络中的广播、组播进行必要的控制。专用网络区和公用网络区采用 MPLS、VPN 技术隔离，专用网络区及公用网络区之间路由不可达，数据不能直接访问。

(4) 安全审计

安全审计日志记录保存时间为半年以上，能根据记录数据进行分析，生成审计报告，相关信息可报送安全管理系统。

2. 城域网

(1) 结构安全

城域网的核心层由两台高性能路由器组成，具有设备冗余，核心设备之间骨干保证对不同路由主备链路进行保护，其链路带宽 10Gbps 满足业务需要。

可以根据接入单位地理位置和数量适当设置汇接节点。

(2) 访问控制

在城域网与用户接入边界及安全等级不同的网络边界配置相应的访问控制策略。

公用网络区域互联网接入区等之间需要进行数据交换时，采用防火墙、路由控制等安全措施，对交换数据进行病毒扫描和审计。

3. 用户接入

每个接入单位通过安全接入网关控制，实现可以访问但不能同时访问政务外网和互联网。

(二) 业务方面

1. 公用网络区

(1) 结构安全

公用业务服务器采用统一规划的 IP 地址，保证跨部门、跨地区业务的交换与共享。根据所部署系统的重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，按照方便管理和控制的原则为各子网、网段分配地址段。按照业务服务的重要次序指定带宽分配优先级别，保证在网络发生拥塞时优先保护重要业务的畅通。

(2) 访问控制

通过互联网或其他公众通信网络对公用网络区的信息系统进行远程访问时，采用 VPN 网关、身份认证、IP 地址绑定、审计等安全措施。通过身份认证、授权管理系统等对公用网络区的信息系统进行保护。

2. 互联网接入区

对互联网接入区的信息系统或服务器进行远程维护和管理，采用身份认证、指定管理终端等安全措施。能有效防止攻击行为：病毒攻击、端口扫描、木马后门、拒绝服务、缓冲溢出、IP 碎片、SQL 注入、蠕虫攻击和蠕虫攻击等。具备流量分析控制、异常告警灯功能，能区分 HTTP、FTP、TELNET、SMTP、POP3、P2P 等各类网络协议并进行安全控制。此外，本项目还从物理安全、网络安全、主机安全、应用安全、数据安全、终端安全和安全管理体系等加强系统安全防护。

1. 物理安全

物理环境安全目的是保护网络中计算机网络通信有良好的电磁兼容工作环境，并防止非法用户进入计算机控制室和各种偷窃、破坏活动的发生。物理安全主要涉及环境安全（防火、防水、防雷击等）、设备和介质的防盗防破坏等方面。具体包括：机房选址、物理访问控制、防盗窃和防破坏、防雷、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等。

本项目的机房改造内容包括：空调系统及新风系统、机房综合布线系统、机房环境监控系统等，详见机房及配套工程建设章节。机房的物理环境基本能满足等级保护三级的要求。

2. 网络安全

网络安全防护将综合采用多种成熟的安全技术，在网络结构、访问控制、安全审计、入侵防范等多方面对信息系统进行安全保障。

（一）网络结构安全

核心设备关键部件如引擎、电源、风扇等均可支持冗余热插拔。根据业务特点和安全需求划分安全区域：业务终端与业务服务器区之间进行路由控制。

（二）访问控制

在各个网络区域边界，分别部署防火墙进行安全隔离和访问控制，支持链路状态检测，支持基于源地址/目标地址、协议和端口号的访问控制，支持 3 层以下的网络攻击防护。在国际互联网出口边界部署防火墙，在具备传统防火墙功能的基础上还支持基于应用、用户行为的访问控制，支持基于应用的流量管理，实现对应用带宽的有效控制。

（三）安全审计

部署 1 套网络安全审计系统，集成身份认证、基于角色的访问控制及网络内容审计为一体，通过网络旁路侦听的方式对网络数据流进行采集、分析和识别，并对应用层协议进行完整还原，根据制定的安全审计策略进行审计响应，对业务系统核心系统

和核心应用系统实现 命令级别、访问逻辑级别的认证和审计。审计系统支持网站访问行为审计、邮件审计、论坛审计、即时通讯审计、文件上传下载审计、业务操作监控、数据库审计、网络应用行为审计、流量审计等。

(四)入侵防范

互联网接入区配置防火墙并启用入侵检测功能。公用网络区边界部署1套网络入侵检测系统(IDS)。采用全面深入的协议分析技术,结合模式匹配、协议识别、协议异常检测、关联分析等多种技术,准确识别各种攻击,能够检测接近 100 种的网络应用层协议;支持检测蠕虫、网络病毒,包括 Santy、Witty、Mydoom、Sasser、MS Blaster、SQL Slammer、Nimda 以及 Code-Red 等,支持检测间谍软件,包括冰河木马、流光广外女生木马、Netspy 木马、NetBus 木马等,支持检测常见攻击行为,包括溢出攻击、暴力破解、SQL 注入、DOS、扫描等攻击行为等;提供丰富的入侵阻断和响应方式,包括丢弃数据包、丢弃会话、控制台告警、Email、日志数据库记录、snmp trap、防火墙联动、打印机以及用户自定义的行为。用于监控可能存在的入侵和攻击行为,实时监控并采集发生的安全事件和安全趋势。

3. 主机安全

实施主机安全策略管理,确保主机的访问控制、账户管理、口令策略、共享与服务、补丁及防病毒软件安装升级等方面的安全。为提高主机系统安全性,保障各种应用的正常运行,对主机系统身份鉴别加固措施,主要包括:

对登陆操作系统和数据库系统的用户进行身份验证,且保证用户名的唯一性,禁止多用户混用一个账号;

通过设备强制设定或通过制度来实现本要求配置用户名/口令,口令必须具备 3 种以上字符、长度不少于 8 位并定期更换;

主机开启安全事件日志,设备启用登陆失败处理功能,登陆失败后采取结束会话、限制非法登陆次数和自动退出等措施;

通过堡垒认证主机对维护管理实现集中认证与授权。管理员在远程时启用 SSH 等管理方式,加密管理数据,防止数据被窃听;

堡垒主机启用双因子认证功能,对主机管理员登陆进行双因数认证方式,采用 USB key+密码进行身份鉴别。部署 IPS 进行入侵防范监测和报警;

开启主机的审计功能,结合网络安全审计系统进行统一审计;

部署网络版的杀毒软件,在所有服务器安装防病毒系统,使其免受病毒侵害;

4. 应用安全

应用安全防护主要包括应用系统的代码开发安全和应用系统投入运行后的安全防护。

(1) 代码开发安全

为确保应用系统的安全，在应用系统开发前就应确认系统的安全需求，并以此作为开发设计各阶段的基础。在系统开发各个阶段包括需求分析、设计、开发、维护及最后的文档编写等应遵守各种安全规范。应用系统的开发应遵循下面的原则，以确保开发过程中的安全。

- 1) 系统开发应从业务需求的角度出发，不得盲目追求系统的先进性而忽略了系统的实用性。系统的开发是为了更好地满足业务上的需要，而不是技术上的需要。
- 2) 开发的方法和管理必须规范化、合理化、制度化，从而确保开发的质量和进度。
- 3) 应保证开发的进度并按时完成。确保开发工作及时、有效且高质量的完成。
- 4) 系统开发必须具有一定的前瞻性，符合主流系统的发展方向。
- 5) 提高和加强开发人员的安全意识。确保信息和关键技术不会泄漏。

(2) 安全防护

通过部署在国际互联网出口的下一代防火墙进行应用安全防护。

5. 数据安全

对核心路由器、交换机等关键硬件设备和链路采用冗余构架进行建设，并对配置进行数据备份。

6. 终端安全

利用网络防病毒系统对办公终端进行病毒系统集中安装、升级管理。部署政务外网终端安全管理系统，实现对办公终端的移动存储管理、补丁检测审计与补丁分发、客户端防病毒软件安装升级管理、终端桌面安全管理及审计等。

7. 安全管理体系

安全管理体系设计主要是依据《信息系统安全等级保护级别要求》中的管理要求建设，具体包括：

安全管理机构

安全管理机构的任务包括统一规划各级网络系统的安全，制定完善的安全策略和措施，协调各方面的安全事宜等。根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责：

设置安全管理岗位、设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员分配，成立指导和管理信息安全工作的委员会或领导小组，其最高领导

由单位主管领导委任或授权；指定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求；建立授权与审批制度；建立内外部沟通合作渠道；定期进行全面安全检查，特别是系统日常运行、系统漏洞和系统设备备份等。

(二) 安全管理制度

安全管理制度体系是规范和指导安全管理活动的一整套完善、严密、纵横联系的程序和方法，以确保人人各司其职，各尽其责，忠于职守，勤奋工作，各项信息安全活动做到规范化、高效率化，并各职能部门和环节之间分工、协调地进行，从而建立起全网安全保障机制。主要安全管理规章制度如下：

(1) 物理与环境安全管理制度

1) 场地与设备安全管理制度。包括：机房物理位置防护、安全物理控制、防火、防水、防盗、防雷击、机房保护（如：采用屏蔽机房等）等配套设施，以及出入控制等管理制度。

2) 设备、线路、电源管理制度：包括：设备的采购、保管、使用、保养、维修制度。

3) 存储介质管理制度：包括媒体数据管理制度。

(2) 系统安全管理制度

1) 安全设备管理制度：包括对防火墙、IDS、漏扫等的设置、调整和审计进行管理。

2) 虚拟专网管理制度：根据业务、区域划分 VPN，对 VPN 的设置、调整和运行进行管理。

3) 软件系统管理制度：包括操作系统、数据库管理系统、数据共享库监控、应用软件系统和网络管理软件的运行、维护管理制度。

4) 网络资源备份管理制度：包括对网络所有资源进行冗余备份管理等。

(3) 网络运行安全管理制度

1) 安全管理中心管理制度：对网络进行实时监控，并对特征库定期升级。

2) 计算机病毒防治管理制度：包括全网统一防杀病毒、定期升级病毒库等制度。

3) 信息备份管理制度：对信息资源进行备份，包括异地备份、自动备份、人工备份等制度。

(4) 信息安全保密管理制度

1) 身份识别和密钥管理制度：包括用户登录管理制度(电子钥匙和电子令牌管理、指纹库管理等)，用户身份识别管理制度(对上网用户进行身份验证，并根据用户权限发放电子证书等)等。

2) 访问权限管理制度：对用户权限进行管理。

3) 安全审计管理制度：对用户操作进行审计，记录重要的和违规的操作等。

4) 内部评估制度：定期对网络进行安全漏洞扫描，对漏洞进行修补，并定期升级漏洞库等。

5) 人员管理制度：包括用户行为规范、岗位人员标准、人员的聘用与解聘、岗前培训与上岗制度、安全宣传教育管理制度。

8. 其他注意事项

1) 安全产品采购和使用

①安全产品采购和使用应符合以下要求：

②应确保安全产品采购和使用符合国家的有关规定；

③应确保密码产品采购和使用符合国家密码主管部门的要求；

④其同一类别的安全产品原则上应采用同一品牌的产品。

2) 安全服务商选择

①安全服务商选择应符合以下要求：

②应确保安全服务商的选择符合国家的有关规定；

③安全服务商应具备国家相关部门颁发的安全服务资质证书；

④应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

10.3.7.4 备份系统建设方案

10.3.7.4.1 全网备份

通过备份软件，实现整个业务系统的全网备份，实现D-D-T的三层备份体系结构，可以对业务关键数据实现离线保护和快速恢复；根据内外网隔离的特性，实现分区备份，集中管理。

10.3.7.4.2 应用服务器安全

对整个数据中心的应用服务器进行保护，一旦应用服务器发生故障，造成服务停止，可以通过在线应用保护系统恢复应用服务器，对外提供服务。

10.3.7.5 运行维护系统建设方案

10.3.7.5.1 运维系统总体规划

电子政务外网项目运维支撑系统分为三个子系统： 监控管理子系统、资源管理子系统和运维管理子系统。在具体实现上，遵循国家电子政务外网的功能和接口规范要求。电子政务外网运维支撑系统总体功能结构如下图所示：



运维支撑系统总体架构图

1. 监控管理子系统

监控管理子系统主要包括对网络、网络单元进行静态信息的采集，故障和性能监视，采集相关的故障和性能表征参数，评价网络和网络单元的状态和有效性，支持网络分析和网络规划。监控管理子系统能够显示拓扑结构，并提供拓扑节点的级联菜单，为运维人员提供综合性的网络信息显示功能。

2. 资源管理子系统

资源是指需要独立进行分配、维护和监控，且具有配置、性能和故障等信息的物理或逻辑对象。资源管理子系统主要用于管理政务外网相关资源，提供相关资源的配置信息，掌握各种资源的配备及使用情况，对资源进行统一规范管理。

3. 运维管理子系统

运维管理子系统用于运维支撑系统的统一维护管理工作，它主要提供两大类管理功能：面向服务流程的管理功能和面向运维生产的管理功能。运维管理子系统通过流程管理和工单管理的支撑使日常的运维工作流程化，职责角色清晰化，还可以保留业务痕迹为业务统计、考核、监督提供基础数据。

10.3.7.5.2 总体技术方案

运维支撑系统采用分层设计方法：

1. 数据采集层

数据采集主要完成从各个被管对象，获取它们的性能、告警以及配置信息的功能。采集对象是根据系统管理对象，分为平台类和应用类对象，包括网络、主机、数

据库、中间件、存储备份以及应用系统自身状态采集等。采集内容是采集被管对象的信息类型，包括性能、告警、配置信息的采集。

2. 功能层

从系统架构设计角度，功能层除了包括监控模型子系统、资源管理子系统、运维管理子系统三个业务系统外，还包括管理系统本身的相关用户及其访问权限的权限管理子系统，以及提供开放、标准、规范接口功能的接口子系统。各子系统由数据流和工作流提供基础支撑、互相调用。

3. 展现层

大电子政务外网运维支撑系统统一接入门户是系统各类用户获取系统功能与服务的入口和交互界面，为各类用户提供了一个统一的应用操作平台，通过统一的安全认证和授权管理，可实现对各种应用服务的安全访问。使用者可以在统一的用户界面上对业务支撑网的应用部件和平台部件进行集中监控、集中维护与集中管理，实现多点接入、单点操作。

10.3.7.5.3 部署方案

1. 部署方式

电子政务外网运维支撑系统采用集中部署方式，运维人员通过远程登录系统的方式，实现对网络的运行监控。

2. 监控范围

电子政务外网网管监控系统的监控对象包括：县级横向城域网所有网络设备、安全设备、服务器和系统软件。

10.3.7.5.4 运维范围

1. 路由设备。系统需要的主机数目较多，各类硬件可能出现问题，包括路由器、交换机、网络服务器主机、数据库服务器等，定期保养和提供相应配件。

2. 病毒防护。防毒软件、防火墙等也要定期进行更新补丁，并且保证病毒库是最新的，定期进行病毒扫描、木马查杀等工作。

3. 网管设备。定期将交换机、防火墙、网络服务器主机、数据库服务器等的各项指标信息收集集中，以报表形式呈现，以及早发现问题。

4. 网络维护。定期测算系统网络速度、数据流量，提前做好服务器扩容等准备工作，保证系统正常有效地工作。

10.3.8 主要选型原则配置

10.3.8.1 系统配置及软硬件选型原则

设备选型配置上遵循先进实用、稳定可靠、兼容开放、满足要求的原则，优先选用自主可控知识产权的设备，保障系统顺利实施与稳定运行。

(一) 网络设备选型原则

1. 所选用的关键设备具备电信级设备能力，全部网络设备均符合国家和国际标准，具有国家颁发的网络设备入网证件。

2. 网络设备在技术上具有先进性和成熟性。

3. 网络设备自身具有一定的安全防护特性，所选用的网络设备应提供一定的自我安全防护功能。

4. 良好的可扩展能力和互联互通互操作特性，达到国家的互联互通要求。

5. 良好的管理性能。

6. 使用自主可控的国产化设备。

7. 性能优良、配置合理、具备良好的性能价格比和扩充能力。

(二) 安全设备选型原则

1. 关键设备具备电信级设备可靠性能力，党政机关部署的信息网络设备和应用系统必须是安全可靠的。通用设备应当选用政府采购目录中的国产产品，安全保密产品必须经过保密安全检测并符合保密规定和标准，密码产品应当选用国家密码管理部门批准的产品，病毒防护产品应当选用公安机关批准的国产产品。。

2. 具有良好的可扩展能力和互联互通互操作特性。

3. 技术成熟、性能先进、使用可靠。

4. 产品高度智能化、技术含量高，并具有良好的管理性能。

5. 性能稳定、配置合理、具备良好的性能价格比。

6. 满足国家对安全的要求。

7. 优先使用国产设备。

(三) 服务器设备选型原则

1. 按照先进、实用的原则、采用成熟的技术和开放体系结构。

2. 系统具有高可靠性、高可用性、高服务性。

3. 性能优良、配置合理、具备良好的性能价格比和扩充能力。

4. 选择技术领先、市场和技术前景好的厂家的产品。

(四)主要软件选型原则

1. 适用性好，满足需求

主要考虑根据项目的需求选择最适用的软件，特别注意专用需求的满足程度，同时考虑有利于实施并使二次开发工作量最小。

2. 开放性

主要考虑了操作系统的开放性，以及软件产品本身的开放性，即与其它软件产品的兼容、衔接。

3. 先进性。

4. 商品化程度及应用效果。

5. 软件商对用户可提供的支持程度。软件商对用户可提供的支持直接影响实施进程，判断软件商支持力量的强弱，主要看能否针对用户需求提出有针对性的措施和对用户提出问题解答和解决的满意程度，二要了解技术支持人员的实际经验。

6. 性能价格比。

7. 使用方便性、稳定性。

10.3.8.2 系统部署方案

在公用网络部署杀毒软件、业务监控运维平台以及 DHCP、DNS 等，安全审计系统、入侵检测系统、服务器汇聚交换机以及防火墙等；在互联网区部署出口路由器、防火墙、入侵防御等。

10.3.9 机房设计

10.3.9.1 设计原则

1. 标准性。严格按照国家和行业关于计算机机房的有关标准设计。

2. 先进性。在满足可靠性和实用性的前提下，采用先进的技术和设备，使机房系统达到或接近国际国内先进水平，确保机房系统长期有效的运行。

3. 可靠性。在意外情况下的抗干扰性和快速补充性，保证各个环节都安全可靠。

4. 实用性。在充分考虑机房系统功能完善的基础上，使其性价比达到最优。

5. 整体性。机房工程是一个整体，应充分考虑各系统的布局、格调、色调及效果的一致性和整体性。

6. 扩展性。在满足现阶段的需求上，还能在空间布局、系统容量、配电容量等方面有充分的扩展余地，便于系统可进一步开发及适应未来的更新换代。

7. 安全性。机房的设计与建设必须确保机房的安全可靠，充分考虑防水、防火、防盗、防雷、防干扰、电力故障、通讯故障、非法入侵、降噪、接地及地面承重等安全问题并采取有效措施。

8. 可管理性。采用的各类机房设备应具有智能化、可管理的能力，能通过建立全面、完善的集中监控和管理系统，实时监视机房的运行状况，能及时发现异常情况和故障，提高机房运行的安全性和可靠性。

9. 人机工程。在机房设计和建设过程中应根据人机工程原理，考虑机房工作人员的便利、舒适。

10.3.9.2 设计目标

机房建设目标是建立一个高效、节能、安全、稳定、绿色环保、具有高可靠性、高经济性、高扩展性、高可用性、高可管理性的机房。

10.3.9.3 设计方案

装修工程、电气配电、防雷接地、综合布线、消防、空调新风、安防、环境监控等。

1. 机房区域划分

机房区域划分为主机房区、电池区和监控区。主机房区主要用于放置机柜、布线架、空调、消防设备等；电池区主要用于放置 UPS、配电柜等；监控区主要用于放置监控显示屏、桌椅等辅助设备。机房区域划分需考虑以下 5 点：

- (1) 尽量增加主机房有效面积的利用率，便于机房设备、服务器机柜的合理摆放。
- (2) 机房平面和空间布局应具有灵活性，便于设备增容或区域扩建。
- (3) 尽量合并和减少辅助机房区域面积，提高主机房利用面积。
- (4) 出口通道合理布局，便于机房管理人员、维护、参观访问人员合理分流，体现机房整体的美观形象。
- (5) 便于设备摆放和人员操作，满足空调制冷、配电的需求。

2. 机房装修

(1) 防静电活动地板

1) 机房地板规格 600*600*35mm，敷设高度400mm；均布荷载：1000KG/平方米；集中荷载：200KG；电阻抗 $\leq 10^7\Omega$ 。

(4) 防雷系统

机房雷电防护应当符合《建筑物电子信息系统防雷设计规范》A级标准。

电源线路防护

- 1) 在机房大楼总配电箱处安装一台箱式电源防雷器，作为机房电源一级防雷保护。第一防护区之后的各分区交界处安装Ⅱ型浪涌保护器。
- 2) 在机房楼层配电箱安装一台模块式电源防雷器，作为机房电源二级防雷保护，应配置二端口（串联型）SPD 标称放电电流小于20KA。

地网

根据规范，机房接地系统宜采用联合接地方式，接地电阻应小于等于 4Ω 的要求进行地网设计。

1) 机房接地应优先考虑采用建筑物的自然接地网。联合接地的优点就是尽可能减少雷击时相互连接设备间的电压差，最大可能地实现等电位。机房的接地装置包括机房内接地汇集环、汇集铜排、设备接地线等。

2) 机房接地网(室外人工接地体的设置可为水平带状型、放射型或闭合环型，可根据现场具体情况而定)。

3) 采用接地铜排作为机房接地汇集环排，沿机房四周地板均匀布置(固定在防静电地板下)，采用 BV-50mm² 的铜线作为机房闭合均压接地汇集环；

4) 采用 BV-6mm² 的铜线作为机房内正常工作不带电的金属外壳(如机房的金属门窗、金属吊顶、防静电地板支撑架、设备外壳等)的接地线，接到接地汇集环上；

5) 机房内电源电涌保护器的接地线采用 BV-16mm² 的铜线。接到接地汇集排，长度不宜超过 1 米，信号电涌保护器的接地线采用 BV-4mm² 的铜线与接地汇集环相连，长度不宜超过 1 米；

6) 采用 BV-50mm² 的铜线作为机房接地汇集环引下线，共 2 条，接到机房内的建筑柱主钢筋(采用铜铁过渡接头连接)；

7) 埋设一套抓DK-AGC。电解地极，作为主要降低接地电阻材料。即：为满足该地网接地电阻 $R \leq 4\Omega$ 的技术要求，在地网水平接地线上，均匀布设 DK-AGC 电解地极，通过电解质向地表深层和四周的泄放，将地网改造成半球体，采用等效半球体接地原理进行降低接地电阻。

(5) 综合布线系统

机柜布置

2)活动地板下的地面和四壁装饰,要做平整度处理,保证空调送风系统效率。选用不起尘、不易积灰、易于清洁的材料,做防尘处理后基层采用防尘漆刷二道,并刷防火油漆。

3)为减轻机房空调负荷,降低空调运行费用,防止凝露现象,机房地面要安装保温层,敷设厚橡塑棉保温层,在此基层上表面再铺箔层,起到防尘、保温和允许踩踏的作用。地面垫层宜配筑,维护结构宜采取防结露措施。

4)安装防静电地板时,要求安装静电泄漏系统,活动地板泄露干线采用 BVR-6mm²导线与支架连接,其连接点不少于四处,通过静电泄漏干线和机房安全保护地的接地端子封在一起,将静电泄漏掉。

(2) 动力配电系统

1)机房供电采用三相五线制供电系统,采用双回路供电。频率变化 $50\text{Hz} \pm 0.2\text{Hz}$,电压变化 $380\text{V}/220\text{V} \pm 5\%$,波形失真率小于 $\pm 5\%$ 。机房进线电源由用户拉线到机房门口(三相五线制 16 平方铜芯线);分为三组进电电源(二组为市电供电,一组为备用)。

2)用电设备作接地保护,并入土建大楼配电系统;

3)机房用电设备、配电线路装置过流过载两段保护,同时配电系统各级之间有选择性地配合,配电以放射式向用电设备供电;

4)机房配电系统所用电线为阻燃聚氯乙烯绝缘导线,敷设喷塑桥架、镀锌铁管及金属软管。

5)机房的设备供电和空调照明供电分为两个独立回路,其中设备供电由 UPS 提供并按设备总用电量的 1.3 倍进行预留,而空调照明用电由市电提供并按空调设备的要求供配。

6)机房内的配电系统考虑了与应急照明系统的自动切换。

7)机房设计了一个配电箱,对机房的市电进行配电,配电箱为机房专用标准配电箱,配备 ABB 低压开关。柜内配有市电备用回路,安装防雷保护器。配电箱为机房专用标准配电箱,配备 ABB 低压开关。箱内配有 UPS 电源备用回路,安装防雷保护器。

8)机房所有插座均采用普通电源插座和弹起式铜插座,普通电源插座安装在墙壁上,弹起式电源插座安装在防静电地板上,美观大方。

(3) UPS 系统

UPS 系统在市电和发电机系统停止供电后,在无间断的状况下对原有负荷继续供电。一方面是保证计算机不丢失信息和数据,另一方面是保证设备的安全。机房内电子信息设备采用 UPS 供电线路供电。

1) 服务器机柜每机柜安装的服务器数目以 4-5 台为宜, 配线架间隔 2U, 托盘间隔 6U; 机柜底部为统一的光配线架与电口配线架, 连接至独立配线机柜。

2) 网络机柜设备部署

网络机柜每机柜安装的网络设备, 若大小为 6U-10U, 则不宜超过 2 台; 若大小为 4U, 则不宜超过 4 台; 若大小为 1U, 则不宜超过 8 台; 机柜底部为统一的光口配线架与电口配线架, 连接至独立配线机柜。

3) 电口配线柜设备部署

电口配线柜应独立设置, 其配线架与设备机柜的配线架通过双绞线互连; 电口配线柜安装 1-10 个 48 口 2U 配线架, 间隔为 1U。

4) 光口配线柜设备部署

光口配线柜应独立设置, 其配线架与设备机柜的配线架通过光纤互连; 光口配线柜安装 1-16 个 24 芯 1U 光配线架, 间隔为 1U。

综合布线

机房综合布线系统是机房区域信息传输的纽带, 要保证布线系统的实用性、全面性、可靠性和可维护性。布线系统要求距离尽量短而整齐, 排列有序, 结合“田”字形和“井”字形两种方式。

机房综合布线具体内容有: 强电布线、弱电布线, 其中强电布线和弱电布线均放在金属布线槽内, 布线槽尺寸可根据线量的数量考虑留有余量(一般是 100×50 或者 50×50)。强电线槽与弱电线槽之间的距离应保持至少 5cm 以上, 避免并排敷设, 并采取相应的屏蔽措施, 相互之间不能穿越, 以防止电磁干扰。

1) 强电布线: 在每个机柜和设备附近安排相应的电源插座, 插座的容量为 10A 及 16A。电源的线缆直径应根据电源插座的容量留有一定的冗余。所有强电布线采取过电压保护措施。必须考虑线缆阻燃要求。所有电缆的镀锌金属走线槽或镀锌走线钢管都应该布设在地板下面或吊顶内。

2) 弱电布线: 机房弱电布线主要超五类网线和多模光纤等, 参考标准 TIA942 中的以主配线区域 MDA 为布线管理的核心采用星型结构分布的布线方式, 方便地解决各个设备与路由实际应用与管理。

(6) 空调制冷

在机房中, 诸如环境、温度、湿度、洁净度, 以及工作人员和设备的散热量等都会对计算机及附属设备工作的稳定性、可靠性造成危害。空调系统具有送风、回风、加热、加湿、冷却、减湿和空气净化化的功能, 能维持机房内恒温、恒湿状态, 并控制

机房内的含尘量。因此需要空调来维持特定的温度、湿度和洁净度来保证机房高效的运行。

1) 环境要求

空调系统开机时主机房的温度、湿度应达到《GB50174-2017》机房要求。温度恒定控制在 18℃-28℃，温差 1-2℃之内，湿度恒定控制在 25%-75%，空气洁净度大于等于 0.5 微米/升<18,000，换气次数/小时>30，新风量 30m³/人.小时，机房正压>10Pa。

空调配置

机房主要的热负荷来源于设备的发热量及维护结构的热负荷。如不具备精确计算的条件,也可根据建筑负荷与设备负荷估算法进行测算

(7) 接地系统

接地装置是增强静电泄漏和导流，使带电物体的静电荷得以顺利泄出和迅速导走，以避免静电积聚。

1)采用联合接地。

活动静电地板、饰面金属塑板墙、不锈钢玻璃隔墙等材料均采用导线布成泄漏网，接地电阻应不大于1，并用干线引至动力配电柜中交流接地端子。

2)为防止感应雷、侧击雷沿电源线进入机房损坏机房内的重要设备，在电源配电柜电源进线处安装浪涌防雷器，或者在计算机设备电源处使用带有防雷功能的插座板。

(8) 消防系统

机房消防系统七氟丙烷气体灭火系统，在机房上方采用无管网布置气体消防喷头，在火灾发生时快速对机房设备区域喷射七氟丙烷气体。

机房顶面安装温感及烟感，监视机房火情。自动消防灭火系统具备自动监测火情、自动报警、自动切断电源和启动自动灭火系统设备 或通过其他应急设施，实现消防系统的自动化。

(9) 照明系统

机房内照明装置宜采用机房专用无眩光灯盘，由市电供电，其照度>400LX，市电断电时，通过分电柜中的自动投切装置自动投换UPS 供电作应急照明，其照度>60LX。

(10) 安防系统

机房作为信息系统的核心重地，需要保证绝对的安全，需要建立一个结合视频监控和门禁结合系统，通过指纹读卡器检测并记录开关状态、开门时间、门区及责

任人等统计资料。也可以实时监控到进入机房的人员以及对非法闯入进行报警和录像，为机房的安全提供保障。

(11) 机房维护和管理制度

通过建立规范的运维和管理制度，保证计算机设备的电力持续供应和供电质量与环境符合设备运行要求，同时不断降低运行维护成本。

1) 维护和管理内容

制度的建设要从管理角度明确机房管理工作的原则和工作目标，确立各单位和各部门的工作职责范围，明确工作职责和岗位设置。通过制定机房管理相关办法，明确将机房按照重要性程度进行分类，并制定了不同层次的管理要求。

制度建设要从技术角度，明确机房建设和环境动力设施配备的标准和规格，一方面使机房的建设能够达到统一的设计水平，满足一段时期的使用和发展要求，另一方面能够防止过高标准所带来的资源浪费。

制度建设要从后续的维护角度，明确机房环境设施的技术维护要点和要求，防止出现只重视建设轻视维护管理的局面。通过制订机房相关环境动力设施维护规范，确定机房环境设施的基本维护要求，确保及时发现故障隐患，把问题消灭在萌芽阶段。

2) 管理体系制度

管理体系制度包括三层：第一层：程序手册(工作手册)；第二层：各类操作手册、维护手册、应急手册等；第三层：操作规范、工作流程、操作流程等。

3) 机房管理制度

机房管理制度包括：人员管理、机房规划管理、应急管理、机房安全防范管理、机房监控管理、机房建设技术规范、机房环境设施维护规范等方面。

4) 机房运维制度

机房运维制度包括：机房环境设施维护文档、维护技术管理、维护管理演变、维护工具与材料使用方法、维护档案、维护规范等方面。

10.3.10 政策依据

(1) 《国务院关于加强数字政府建设的指导意见》(国发〔2022〕14号)

(2) 《国家发展改革委关于印发〈“十四五”推进国家政务信息化规划〉的通知》(发改高技〔2021〕1898号)

(3) 中央网络安全和信息化委员会印发的《“十四五”国家信息化规划》

(4) 《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》(国办函〔2022〕102号)

(5)《国务院办公厅关于加快推进政务服务“跨省通办”的指导意见》(国办发〔2020〕35号)

(6)《中央网信办、国家发展改革委、工业和信息化部关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知》(中网办发〔2021〕15号)

(7)《工业和信息化部中央网络安全和信息化委员会办公室关于印发〈IPv6流量提升三年专项行动计划(2021-2023年)〉的通知》(工信部联通信〔2021〕84号)

(8)《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》

(9)《河南省人民政府关于印发河南省“十四五”数字经济和信息化发展规划的通知》(豫政〔2021〕51号)

(10)《河南省人民政府关于印发河南省加强数字政府建设实施方案(2023—2025年)的通知》(豫政〔2023〕17号)

(11)《河南省人民政府办公厅关于印发河南省建立健全政务数据共享协调机制加快推进数据有序共享实施方案的通知》(豫政办〔2022〕62号)

(12)《河南省人民政府办公厅关于加快推进新型智慧城市建设的指导意见》(豫政办〔2020〕27号)

(13)《河南省推进互联网协议第六版(IPV6)规模部署实施计划》

(14)《濮阳市国民经济和社会发展第十四个五年发展规划和2035年远景发展目标纲要》

10.3.11 技术标准

(1)《中华人民共和国网络安全法》

(2)《中华人民共和国个人信息保护法》

(3)《中华人民共和国密码法》;

(4)《中华人民共和国数据安全法》;

(5)《关键信息基础设施安全保护条例》(国令第745号);

(6)《电子政务外网安全接入技术规范》(DB34/T 4283-2022)

(7)《国家电子政务外网IPv6地址规划》(GW0209—2019)

(8)《信息安全技术 网络安全等级保护测评要求》(GBT28448 -2019);

(9)《国家政务服务平台安全接入检测要求》(C0115-2018);

(10)《政务网络安全监测平台总体技术要求》(TC11A 005-2019);

- (11) 《政务网络安全监测平台数据总线结构规范》（T/CIIA 007—2020）；
- (12) 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）；
- (13) 《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）
- (14) 《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）；
- (15) 《信息安全技术网络安全监测基本要求实施指南》（BG/T 36635-2018）；
- (16) 《信息安全技术 电子政务移动办公系统安全技术规范》（GB/T 35282-2017）
- (17) 《国家电子政务外网信息安全标准体系框架》（GW0101-2014）；
- (18) 《国家电子政务外网信息安全标准化工作规范》（GW0102-2014）；
- (19) 《接入政务外网的局域网安全技术规范》（GW0206-2014）；
- (20) 《国家电子政务外网安全接入平台技术规范》（GW0202-2014）；
- (21) 《国家电子政务外网安全管理系统技术要求与接口规范》（GW0204-2014）；
- (22) 《国家电子政务外网安全等级保护实施指南》（GW0104-2014）；
- (23) 《国家电子政务外网跨网数据安全交换技术要求与实施指南》（GW0205-2014）
- (24) 《国家电子政务外网安全监测体系技术规范与实施指南》（GW0203-2014）；

10.4 保密要求

我方提供的线路或相关工作人员严格遵守保密原则，保证政务信息不因线路问题外泄。

10.4.1 项目背景

随着信息化的不断发展，企业所拥有的各类信息也随之增多，其中包括商业机密、客户资源、技术方案等重要信息。这些信息的泄露对企业可能带来极大的经济损失和品牌形象影响，因此，保密工作越来越受到企业的重视。在软件、系统开发等相关领域，为确保信息安全，保密保证措施至关重要。

10.4.2 保密范围

10.4.2.1 保密管理制度

制定完善的保密管理制度，包括保密责任人、保密工作组织机构、保密等级划分、保密审查制度、保密议事规定、保密宣传教育制度等内容，明确公司对涉及保密信息的管理规范。

10.4.2.2 人员安全管理

实行严格的人员安全管理制度，包括招聘前的履历审查、保密意识培训、保密协议签署、岗前培训、定期资格审查等。同时，对于离职人员，应当进行信息安全保障工作。

10.4.2.3 物理环境安全保障

通过实施保密区域划分、机房保密措施、网络接入控制等措施，确保基础设施环境的安全。

10.4.2.4 信息系统安全

实施信息系统安全管理，包括网络安全、数据备份和恢复、安全检测和防护、应急预案制定等内容。同时，对于信息系统的修补漏洞、安全管理制度，进行定期评估和检查。

10.4.2.5 运维团队安全管理

对运维团队进行安全培训、权限管理、审核监管和日常检查，防范泄漏风险。

10.4.3 保密工作流程

针对上述保密保证措施，我司将按照以下工作流程进行合理的保密工作：

10.4.3.1 确认保密信息

在业务流程处理中，公司应该明确哪些涉及保密信息进行分类，只有对重要信息进行优先保障，才能最大程度保证企业的核心竞争力。

10.4.3.2 设定保密等级

设定合适的保密等级，包括绝密、机密、秘密等不同级别，以便于区分保密信息，根据保密等级设定权限控制，达到细致化、人性化管理。

10.4.3.3 文档流程控制

对于涉及保密信息的文件或者数据的书写、存储、传送等，必须为文档加上加密、防护、流程监管等措施。

10.4.3.4 权限控制

根据保密等级，进行权限控制，只让有权限的人员访问信息，严格设定不同人员对信息的访问控制权限。

10.4.3.5 保密审查

在信息流程进行到一定阶段，进行保密审查，避免敏感信息泄露。审查的内容包括：文件个数、文件格式、文件类别、文件大小、机密等级、使用地点、使用人员等信息要求。

10.4.4 保密措施

10.4.4.1 强化保密意识

为从根本上加强工程招标的保密，加强对我公司职工（尤其是项目经理、项目组成员）相关保密知识的学习，加强保密意识。经常组织工作人员对招标投标法、政府采购法、合同法、反不正当竞争法、保密法进行学习，努力做到依法代理，依法招标，严格保密纪律，同时加大对泄密问题的查处，确保招投标活动的公正性、公平性。

10.4.4.2 加强廉政教育和职业道德教育

加强对公司职工的廉政教育和职业道德教育，不断提高公司从业人员的思想觉悟和政治素质，构筑牢不可破的反腐倡廉心理防线，使公司从业人员自觉抵制各种不正之风的侵蚀，积极地预防职务犯罪行为的发生。

10.4.4.3 严格保密制度，加大惩罚力度

凡违反规定，泄露国家、内部秘密、不够刑事处罚的，可视情节严重程度给予通报批评、警告等处分。对有意向外界泄露、出卖内部秘密的人员，将根据危害程度追究经济赔偿或依法起诉。

10.5 网络连续性方案

我公司在项目实施过程中，保证用户业务系统的网络连续性，不得中断业务，并按照用户要求提供完整的技术支持服务和网络连续性方案。

10.5.1 服务范围

名称	参数要求	单位	数量
电子政务网	1、单条宽带100M; 2、速率上行、下行对称; 3、物理链接光纤信号衰减小于等于-26db; 4、采用专线直连的方式。	条	788

10.5.2 建设工期及进度要求

合同签订后，按照项目工期安排进度，我方承诺在15天内完成。

10.5.3 租赁期限

濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目租赁期限1年。

10.5.4 制定完备服务方案

根据用户的实际情况，通过分析现有系统的业务特点和设备运行情况，提供完整的系统服务方案，包括设备巡检计划、维护保养时间计划表、建立各种设备预防性维护保养规程等。同时，还将提供详尽的技术手册，实施严格的项目管理，成立专门的服务团队，指派项目经理作为维保项目负责人，对服务支持实施严格的服务管理，统筹相关工作，以保证维保服务正常高效运行。

10.5.5 服务响应时间

（1）故障报修热线服务

提供7×24小时不间断的电话服务支持，不限次，响应时间不超过10分钟。用户在使用维护范围内遇到问题，都随时可以从我公司得到电话支持与帮助，联系方式：0393-4687010。

（2）远程问题诊断和支持服务

提供7×24小时远程协助支持，响应时间不超过20分钟。若故障不能通过热线支持解决，我公司可使用远程支持服务工具对服务范围内的软件进行远程诊断，或通过其它远程方式为解决问题提供帮助。

（3）现场支持服务

对于通过电话支持和远程支持都不能解决的软件故障，我公司提供7×8小时现场支持服务，安排经验丰富的技术支持工程师赴现场分析故障原因，制定故障解决方案。

现场技术支持完成后，技术支持人员需向用户提交现场技术服务报告，经用户签字确认，双方各自存档。另外针对现场服务相关内容，我公司对用户进行过程解释和现场培训。

我公司将指定一名主要联系人与用户联系。一旦接到用户请求电话，我公司会在规定时间内通过电话解决或远程支持解决用户所提出的问题。我公司因特殊原因需更换指定工程师，会及时通知用户，在用户同意后指定合格的接替人员。

10.5.6 备件更换服务

本项目中涉及到的线路在365天7×24小时范围内，若采购维保服务的设备发生故障需要提供备件时，我公司会在第二个工作日（或12小时内），将完好备件运抵现场，并派工程师在现场完成备件更换，费用由我公司负担。

10.5.7 设备部件调整服务

因工作及业务需要，在保修的系统上增加新的应用或进行数据库等软件的安装与调整等工作时，我公司会派经验丰富的工程师提供电话技术支持，必要时到现场支持，协助用户解决与处理突发事件，以确保系统及业务的正常运行。

如设备需扩容或新增配件时，我公司会派经验丰富的工程师提供电话技术支持，必要时到现场支持，扩容或新增配件费用由用户负担。

10.5.8 技术咨询服务

我公司为用户提供7×8小时数据库、操作系统及网络与安全等多方面的技术支持与咨询服务，我们保证做到主动与用户进行技术交流，提高用户的系统使用能力。

10.6 人员配置及培训

10.6.1 人员配置计划

在保证项目建设质量和进度，保障系统的安全与正常运行维护的前提下合理配置技术人员。根据项目建设期和试运行期间对技术人员的特点和要求的不同以及业务量的多少，根据项目需求来动态调整人员的配置。

根据不同的联网系统设备和环境制定具体的保养方案。包括但不限于符合以下要求。在网络租赁维护期内，我方对于系统故障在1小时内响应，在2小时内确定故障原因和解决方案，在12小时内排除故障，12小时内不能修复的，保证线路稳定运行。配

备10人的专职运行维护和售后服务队伍，制定系统日常维护工作计划，并严格按照工作计划进行系统的日常维护，日常维护不影响系统的正常使用。

10.6.2 人员培训方案

完善的人员培训是一切现代科技应用之基础，也是项目按既定目标实施的关键，针对各个层次的作业人员，通过经验丰富、讲师和教材，施以专业的培训，使我们的实施方案能够发挥最大的效益。通过正规化的现场或异地集中培训，增强各层次的系统使用人员对系统的操作能力和使用能力。

10.6.2.1 培训目的

项目培训的目的是使操作及运维人员更深的了解濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网项目基本理论和方法，经过培训后能够胜任项目的运行管理工作，以保障濮阳市行政审批和政务信息管理局电子政务外网项目的稳定运行。

10.6.2.2 培训目标

通过培训工作的开展，要达到如下目标：

- (1) 操作及运维人员了解指挥中心管理的背景、基本理论和方法；
- (2) 操作及运维人员掌握对多系统、跨平台、跨部门协同管理和运行机制的方法；
- (3) 操作及运维人员熟悉指挥中心管理信息系统的的使用操作；
- (4) 操作及运维人员学会并应用本方案中的指挥中心调度管理机制；
- (5) 操作及运维人员掌握计算机网络系统、数据中心、及其他配套子系统设备的安装、调试和日常维护等操作；
- (6) 操作及运维人员掌握网络安全基本知识，建立网络安全意识；
- (7) 操作及运维人员掌握数据库基本知识，能够进行安装、调试和日常维护。

10.6.2.3 培训时间和地点

培训时间为项目交付验收阶段，共计进行两次集中培训。

培训地点为濮阳市行政审批和政务信息管理局（如有变动双方可以通过协商另行确定培训时间和地点）。

10.6.2.4 培训人员

针对此次项目，我单位会对用户指定人员进行详细的技术培训。

10.6.2.5 培训体系

经过多年的项目实施经验，我单位积极总结了一套成熟的培训体系，其中涵盖了网络系统、网络安全、系统维护、设备连接、故障处理、数据库管理系统、中间件系统、存储、超融合系统、数据备份系统等方面内容。通过系统的、有针对性的培训，可以让系统的使用者、维护者对涉及的问题有系统、全面的了解，以保证用户设备及业务系统的安全、稳定运行。

10.6.2.6 培训方式

(1) 集中培训

集中培训可以在系统推广应用前，组织相关人员（如操作使用人员、系统维护管理人员等）进行。

(2) 现场培训

现场培训可以在系统应用时，由系统技术支持部门提供现场培训服务。

(3) 网络培训

将集中培训和现场培训等内容制作成多媒体课件的形式，用户方技术人员可以通过网络随时、随地通过课件进行学习。通过长期的网络化的培训来更新、强化和深化技术队伍的技术能力。

10.7 售后服务

1、维护期内所有性能指标达到技术规范书的要求时，可按合同约定进行验收。

2、初验后，设备再次经过试运行期，所有性能指标达到技术规范书的要求时，可按合同约定进行下一步验收工作，进行终验。全部达到要求时，采购单位方可签署《濮阳市市级政府采购验收报告》。

3、保修期间供方要保修除消耗品以外的所有产品。如果系统、设备等发生故障，供方要调查故障原因并修复直至满足最终验收指标和性能的要求，或者修理、更换整个或部分有缺陷的材料。

4、保修期内，供方提供电话、电子邮件、Web、现场服务等方式的技术支持，对用户的现场服务要求，供方必须按投标文件做出的承诺进行响应。

5、保修期内，供方应对出现故障无法修复的产品或无法正常运行的系统，提供替代产品以保证系统的正常工作。

6、保修期内，供方应按投标时的承诺提供相关服务。

7、供方必须为维修和技术支持所未能解决的问题和故障提供正式的免费升级方案和升级服务。在质保期内，供方有责任解决所提供的投标货物和软件系统的任何问题；在质保期满后，当需要时，供方仍须对因投标货物本身的固有缺陷和瑕疵承担责任。

8、在保修期结束后，产品在质保期内，供方必须继续提供对产品备件、故障处理、软件升级等的服务，不得以任何借口拖延或中断对产品的售后服务，应说明服务的响应时间、取费标准。

9、供方不能满足以上要求，采购单位有权向供方提出索赔。

10.7.1 售后服务总体目标

我们为本项目制定的总体目标是：

- 1、凭借优秀的售后服务网络，保证系统设备的正常、稳定、不间断地运行；
- 2、依赖公司深厚的技术基础对系统设备进行定期和不定期的巡查和检测，使其永远保持最佳运行状态；
- 3、秉承“客户至上”的立业原则，实时解决用户在系统设备使用中出现的的问题；
- 4、实时响应，“点对点服务”，接到用户质量、服务要求后24小时内正式回复。

10.7.2 总体原则

为了切实做好售后服务工作，我们将遵循以下总体工作原则：

- 1、响应及时性原则：我们将设立项目现场服务小组为用户提供实时响应服务，为项目提供7×24小时全时响应服务；
- 2、服务规范性原则：我们的实施工程师和技术支持、维护工程师具有专业技术技能，严格按照我公司的客户服务规范提供客户服务；
- 3、解决问题高效性原则：遵循解决问题高效性原则，通过现场支持工程师的专业技能快速定位和解决问题。

10.7.3 高效、稳定的服务措施

10.7.3.1 定期现场巡检

在服务期限内将每年安排高级技术人员定期到项目现场进行系统设备检查和维护工作。

10.7.3.2 技术业务咨询与培训

在服务期限内将对本项目的系统管理员和使用人员提供多层次、全方位的技术业务咨询和培训活动，保证系统管理员和系统使用人员在第一时间内得知系统最新信息。

10.7.3.3 企业客户服务中心

公司建立了严格的客户服务体系，保证项目实施的高质量、快进度，对客户服务做到全天24小时快速响应。

10.7.4 持续服务保障措施

项目建设和运转的整个过程离不开技术支持和维护。我们根据招标要求，参照项目的阶段划分，把技术服务和维护工作分为三个阶段，即项目实施阶段、系统保修期阶段以及保修期以后阶段。

10.7.5 项目实施阶段服务保障

这一阶段应包括系统软硬件的订货、运货、提货、交货，设备的安装、调试、测试和培训，以及最后的验收工作。

10.7.5.1 服务方式

这一阶段主要是在客户现场提供服务，现场实时响应客户的要求，保证系统的正常运行。

10.7.5.2 责任和承诺

(1) 保证订货符合工程设计，并按期到位用户指定地点。设备到货前一周内将对系统各接口的相关设备提出具体的硬件、软件、环境等技术要求；

(2) 负责所有合同内的硬件设备的现场安装、调测和运行；

(3) 负责所提供的软硬件设备间的连通，保证多个厂家的同一类型设备的兼容性，保证不同时期所提供的同类设备（硬件、软件）的兼容性；

(4) 承诺提供设备安装调试时所需的设计资料，并在保证安全和质量的前提下向客户方提供技术服务，包括技术咨询、培训等；

(5) 所提供的系统软、硬件设备出现问题或故障时，我公司承诺现场实时响应，免费进行更换和维修；

(6) 验收时我公司将向用户提交测试内容、方法和计划，经用户确认后实行。

10.7.6 保修期阶段服务保障

保修期阶段的特点是系统已经稳定运行一段时间并通过验收了，在具体实施过程中可能忽略的一些问题和隐患随着客户深入使用而逐步暴露，因此系统需要进一步优化。系统维护运行阶段是确保全系统长期正常稳定运行的关键阶段，系统的技术支持和服务也显得尤为重要。这个阶段的主要工作是日常保运、技术交流与培训。

保修期内，由于系统设计、生产、工艺出现的问题，我公司免费负责及时处理，设备硬件和软件故障，免费维修，对不能修复的设备负责免费更换。

10.7.6.1 服务方式

系统有故障时，维修人员将及时赶到现场解决故障；不能修复的，用同类型设备替换，以保障系统正常运行。我公司还提供：免费软件功能升级、故障处理、性能调优、技术咨询、维护和现场巡检等服务，以及其他的技术支持工作。在保修期内，与质保和维修等相关的费用由我公司负责。

10.7.6.2 责任和承诺

- (1) 提供多层次、全方位的技术业务咨询和培训活动；
- (2) 系统软、硬件设备出现问题或故障时，我公司承诺现场实时响应，根据合同规定进行更换和维修；
- (3) 提供高级工程师定期巡检服务；
- (4) 及时提供系统软硬件升级的信息，并对系统软硬件升级提供现场技术支持服务；
- (5) 定期检测系统，系统性能优化服务。

10.7.7 保修期后的服务保障

质保期结束后，我公司仍提供与保修期内相同质量的售后服务，且只收取成本费用（含零件等）。

保修期阶段的特点是系统已经稳定较长时间，免费服务已经履行完毕，客户可以有选择性地选择合适的服务来保证系统的生命周期的延续。可选择服务：

- 免费提供电话支持、远程在线支持、技术咨询服务；
- 多层次、全方位的技术业务咨询和培训活动；
- 系统软、硬件设备更换和维修；
- 高级工程师定期巡检服务；
- 系统软硬件升级现场技术支持服务；
- 定期检测系统，性能优化服务。

10.7.8 售后运维服务承诺

(1) 网络租赁维护期内，若我方中标，我方承诺：将对于系统故障在1小时内响应，在2小时内确定故障原因和解决方案，在12小时内排除故障，24小时内不能修复的，保证线路稳定运行。

(2) 我方配备10人的专职运行维护、售后服务队伍。

(3) 制定系统日常维护工作计划，并严格按照工作计划进行系统的日常维护。日常维护应不影响系统的正常使用。

(4) 客户方要求的其他内容，具体以后期合同约定。

