

招标文件

|  |  |
| --- | --- |
| 项目编号： | LCZ2021-016 |
| 项目名称： | 丽水市电子政务网络及数据安全服务项目 |
| 采 购 人： | 丽水市大数据发展管理局 |
|  |  |
|  |  |
| 采购代理机构： | 丽水市公共资源交易中心 |
| 地 址： | 丽水市人民街615号商会大厦5楼 |
|  |  |
| 2021年9月 | |

目 录

[目 录 1](#_Toc81474744)

[第一章 招标公告（邀请） 1](#_Toc81474745)

[第二章 招标需求 4](#_Toc81474746)

[一 产地要求 4](#_Toc81474747)

[二 采购内容及清单 4](#_Toc81474748)

[三 执行标准要求： 4](#_Toc81474749)

[四 技术需求 4](#_Toc81474750)

**[（一）项目背景](#_Toc81474751)** [5](#_Toc81474751)

**[（二）技术需求](#_Toc81474752)** [5](#_Toc81474752)

[五 商务要求 57](#_Toc81474753)

**[（一）服务期](#_Toc81474754)** [57](#_Toc81474754)

**[（二）服务要求](#_Toc81474755)** [57](#_Toc81474755)

**[（三）付款方式](#_Toc81474756)** [57](#_Toc81474756)

[六 安装、调试、验收要求 58](#_Toc81474757)

**[（一）供货（安装）地点要求](#_Toc81474758)** [58](#_Toc81474758)

**[（二）项目人员要求](#_Toc81474759)** [58](#_Toc81474759)

**[（三）项目实施计划要求](#_Toc81474760)** [58](#_Toc81474760)

**[（四）项目验收](#_Toc81474761)** [58](#_Toc81474761)

**[（五）服务绩效要求](#_Toc81474762)** [59](#_Toc81474762)

[七 讲解演示要求 61](#_Toc81474763)

**[（一）讲解](#_Toc81474764)** [61](#_Toc81474764)

**[（二） 演示](#_Toc81474765)** [61](#_Toc81474765)

[八 其他 62](#_Toc81474766)

[第三章 投标人须知 63](#_Toc81474767)

[投标人须知前附表（一） 63](#_Toc81474768)

[投标人须知前附表（二） 65](#_Toc81474769)

[一 总则 66](#_Toc81474770)

[1.1 适用范围 66](#_Toc81474771)

[1.2 定义 66](#_Toc81474772)

[1.3 投标人应具备资格条件 66](#_Toc81474773)

[1.4 联合体 67](#_Toc81474774)

[1.5 投标文件的语言及计量 67](#_Toc81474775)

[1.6 投标费用 67](#_Toc81474776)

[1.7 现场踏勘 67](#_Toc81474777)

[1.8 答疑会 67](#_Toc81474778)

[1.9 分包 68](#_Toc81474779)

[1.10 保密 68](#_Toc81474780)

[1.11 政府采购政策 68](#_Toc81474781)

[1.12 信用信息记录查询 69](#_Toc81474782)

[1.13 质疑和投诉 69](#_Toc81474783)

[1.14 特别声明 70](#_Toc81474784)

[二 招标文件 70](#_Toc81474785)

[2.1 招标文件的组成 70](#_Toc81474786)

[2.2 招标文件的澄清、修改 71](#_Toc81474787)

[三 投标文件 71](#_Toc81474788)

[3.1 投标文件的形式和效力 71](#_Toc81474789)

[3.2 在线投标响应（电子投标）说明 71](#_Toc81474790)

[3.3 投标文件组成 72](#_Toc81474791)

[3.4 资格审查文件的组成 72](#_Toc81474792)

[3.5 资信商务及技术文件的组成 72](#_Toc81474793)

[3.6 报价文件的组成 72](#_Toc81474794)

[四 投标文件的编制 72](#_Toc81474795)

[4.1 投标文件编制 72](#_Toc81474796)

[4.2 投标报价要求 73](#_Toc81474797)

[4.3 投标有效期 73](#_Toc81474798)

[4.4 投标文件格式 73](#_Toc81474799)

[4.5 投标文件份数及签署 73](#_Toc81474800)

[五 投标文件的提交 73](#_Toc81474801)

[5.1 投标文件导入和加密 73](#_Toc81474802)

[5.2 投标文件的提交 74](#_Toc81474803)

[5.3 投标文件修改和撤回 74](#_Toc81474804)

[5.4 备选投标方案 74](#_Toc81474805)

**[5.5 投标诚实信用](#_Toc81474806)** [74](#_Toc81474806)

[六 开标和评标 75](#_Toc81474807)

[6.1 开标 75](#_Toc81474808)

[6.2 资格审查 75](#_Toc81474809)

[6.3 评标 76](#_Toc81474810)

[6.4 投标文件的澄清、说明或补正 77](#_Toc81474811)

[6.5 报价错误修正 78](#_Toc81474812)

[6.6 评标报告 78](#_Toc81474813)

[七 ▲投标无效的情形 79](#_Toc81474814)

[7.1 在开标时，如发现有以下情形之一的，其投标无效 79](#_Toc81474815)

[7.2 在符合性审查时，如发现下列情形之一的，其投标无效 79](#_Toc81474816)

[7.3 在资信商务技术评审时，如发现下列情形之一的，其投标无效 79](#_Toc81474817)

[7.4 在报价评审时，如发现下列情形之一的，其投标无效 79](#_Toc81474818)

[7.5 如有下列情形之一的，其投标无效 80](#_Toc81474819)

[7.6 如有下列情形之一的，可中止电子交易活动的情形 80](#_Toc81474820)

[八 中标和合同 81](#_Toc81474821)

[8.1 中标 81](#_Toc81474822)

[8.2 中标公告和中标通知书 81](#_Toc81474823)

[8.3 履约保证金 81](#_Toc81474824)

[8.4 合同 82](#_Toc81474825)

[九 其他事项 82](#_Toc81474826)

[9.1 解释权 82](#_Toc81474827)

[第四章 合同格式 83](#_Toc81474828)

[第五章 投标文件格式 93](#_Toc81474829)

[一 资格审查文件格式 93](#_Toc81474830)

[1.1 资格审查文件封面格式 93](#_Toc81474831)

[1.2 资格审查文件目录 94](#_Toc81474832)

[1.3 有效营业执照复印件 94](#_Toc81474833)

[1.4 负责人身份证复印件 94](#_Toc81474834)

[1.5 授权委托书格式 95](#_Toc81474835)

[1.6 具有良好的财务会计制度、依法缴纳税收和社会保障资金的承诺函格式 96](#_Toc81474836)

[1.7 具有履行合同所必需的设备和专业技术能力承诺函格式 96](#_Toc81474837)

[1.8 无重大违法记录声明书格式 97](#_Toc81474838)

[1.11 特定资格条件证明材料附件（若有） 98](#_Toc81474839)

[1.12 其他 98](#_Toc81474840)

[二 资信商务及技术文件格式 99](#_Toc81474841)

[2.1 资信及商务文件封面格式 99](#_Toc81474842)

[2.2 资信商务及技术文件目录 99](#_Toc81474843)

[2.3 投标函格式 100](#_Toc81474844)

[2.4 投标人资质 102](#_Toc81474845)

[2.5 成功案例及业绩及相关证明材料格式 102](#_Toc81474846)

[2.6 服务需求理解分析 102](#_Toc81474847)

[2.7 服务能力 102](#_Toc81474848)

[2.8 安全监管平台服务方案 103](#_Toc81474849)

[2.9 网络安全一体化支撑平台服务 103](#_Toc81474850)

[2.10 网络安全基础服务 103](#_Toc81474851)

[2.11 网络安全加固服务 103](#_Toc81474852)

[2.12 数据安全一体化支撑平台服务 104](#_Toc81474853)

[2.13 数据安全基础防护服务 104](#_Toc81474854)

[2.14 安全运行服务 104](#_Toc81474855)

[2.15 安全体系保障服务 104](#_Toc81474856)

[2.16 拟投入的项目班子格式 105](#_Toc81474857)

[2.17 投标人需要说明的其他文件和说明 105](#_Toc81474858)

[三 报价文件格式 106](#_Toc81474859)

[3.1 报价文件文件封面格式 106](#_Toc81474860)

[3.2 报价文件文件目录 106](#_Toc81474861)

[3.3 开标一览表格式 107](#_Toc81474862)

[3.4 报价明细表格式 108](#_Toc81474863)

[3.5 中小企业声明函格式 109](#_Toc81474864)

[3.6 残疾人福利性单位声明函格式 110](#_Toc81474865)

[3.7 监狱企业证明格式 111](#_Toc81474866)

[第六章 评标办法和细则 112](#_Toc81474867)

[一 总则 112](#_Toc81474868)

[二 评审一般规定 112](#_Toc81474869)

[三 评审内容及标准 112](#_Toc81474870)

[附件：政府采购活动现场确认声明书 115](#_Toc81474871)

第一章 招标公告（邀请）

项目概况：

丽水市电子政务网络及数据安全服务项目 的潜在投标人应在浙江政府采购网（**zfcg.czt.zj.gov.cn**），丽水市公共资源交易网（**lssggzy.lishui.gov.cn**）采购公告附件中自行获取招标文件，并于2021年9月24日09：00（北京时间）前提交投标文件。

**一、项目基本情况**

项目编号：LCZ2021-016

项目名称：丽水市电子政务网络及数据安全服务项目

采购方式：公开招标

采购需求：见采购文件第二章

**标项一**

数量：3

单位：年

预算金额：2020万元

最高限价：2020万元

简要规格描述：见采购文件第二章

备注：无

合同履行期限：3年

联合体投标：□接受 ☑不接受

**二、申请人的资格要求**

1. 满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”网站（**www.creditchina.gov.cn**）、中国政府采购网（**www.ccgp.gov.cn**）列入失信被执行人、重大税收违法当事人名单、政府采购严重违法失信行为记录名单；

2. 落实政府采购政策需满足的资格要求：无

3. 本项目的特定资格要求：无

**三、获取招标文件**

1. 时间：发布公告之日至2021年9月24日，每天上午00：00至12：00，下午12：00至23：59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

2. 地点（网址）：浙江政府采购网（http：//zfcg.czt.zj.gov.cn），丽水市公共资源交易网（http：//lssggzy.lishui.gov.cn）公告附件

3. 方式：自行下载获取

⑴获取流程：浙江政府采购网—用户入驻/登录—用户登录—项目采购—获取招标文件管理；

⑵未在浙江省政府采购网（zfcg.czt.zj.gov.cn）注册成为正式供应商的，请注册完成审核成功后方可登录获取，注册流程见网址：[zfcg.czt.zj.gov.cn/register/2017-07-24/6728.html?\_=2020-03-09%2006：](http://zfcg.czt.zj.gov.cn/register/2017-07-24/6728.html?_=2020-03-09%2006:00:22)[00：22](http://zfcg.czt.zj.gov.cn/register/2017-07-24/6728.html?_=2020-03-09%2006:00:22)，注册咨询电话：400-881-7190；

⑶在浙江政府采购网采购公告附件中以“游客”身份（或丽水市公共资源交易网）获取的招标文件在仅供阅览；潜在供应商未按上述第⑴条方式获取招标文件的不得对招标文件提起质疑投诉；

4. 售价：0元

**四、提交投标文件截止时间、开标时间和地点**

1. 提交投标文件截止时间：2021年9月24日 09：00（北京时间）

2. 投标地点（网址）：

⑴ 电子加密投标文件：在“政府采购云平台”上传提交，“电子加密投标文件”成功上传提交后，投标人自行打印投标文件接收回执；

⑵备份投标文件：投标人自行确定是否提交；若提交请将备份投标文件以电子邮件的形式发送至（lssggzyjyzx@163.com），备份投标文件在“电子加密投标文件”在线解密失败后启用，否则不予以启用；未在规定时间内发送备份投标文件造成的响应无效或失败由供应商自行承当。

3. 开标时间：2021年9月24日 09：00（北京时间）

4. 开标地点（网址）：浙江政府采购网—用户入驻/登录—用户登录—项目采购—开标评标—进入开标大厅

**五、公告期限**

自本公告发布之日起5个工作日。

**六、其他补充事宜**

1. 投标人认为招标文件使自己的权益受到损害的，可以自获取招标文件之日或者招标文件公告期限届满之日（公告期限届满后获取招标文件的，以公告期限届满之日为准）起7个工作日内，以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

2. 其他事项：本项目全程电子招投标，相关的操作规程务必关注《政府采购项目电子交易管理操作指南-供应商》（网址：https：//service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na）

**七、凡对本次招标提出询问、质疑、投诉，请按以下方式联系**

1. 采购人信息

名 称：丽水市大数据发展管理局

地 址：丽水市莲都区人民街615号9楼

传 真：/

项目联系人（询问）：胡春辉 项目联系方式（询问）：0578-2091976

质疑联系人：朱坚 质疑联系方式：0578-2091985

2. 采购代理机构信息

名 称：丽水市公共资源交易中心

地 址：丽水市人民街615号商会大厦5楼

传 真：0578-2292507

项目联系人（询问）：邓茜之 项目联系方式（询问）：0578-2179551

质疑联系人：刘晓华 质疑联系方式：0578-2292511

3. 同级政府采购监督管理部门

名 称：丽水市财政局政府采购监管处

地 址：丽水市莲都区北苑路190号（丽水市财政局）

传 真：0578-2669165

联系人：吴先生、叶先生 监督投诉电话：0578-2669165

若对项目采购电子交易系统操作有疑问，可登录政采云（https：//www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线400-881-7190获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

第二章 招标需求

**一 产地要求**

根据法律法规，本项目采购产品须为中华人民共和国境内（不含港、澳、台）生产或组装。

**二 采购内容及清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **数量** | **单位** | **预算金额（万元）** | **最高限价（万元）** | **备注** |
| 1 | 丽水市电子政务网络及数据安全服务项目 | 3 | 年 | 2020.00 | 2020.00 | / |

**三 执行标准要求：**

1.遵守国家和省市县相关法律规范、技术标准的要求。

2.《中华人民共和国网络安全法》

3.《关键信息基础设施安全保护条例（征求意见稿）》

4.《浙江省深化“最多跑一次”改革推进政府数字化转型工作总体方案》

5.《浙江省数字化改革总体方案》

6.《省大数据局关于一体化智能化公共数据平台方案》

7.《浙江省公共数据和电子政务管理办法》省政府令354号

8.《浙江省公共数据开放与安全管理暂行办法》(省政府令第381号)

9.《浙江省公共数据安全管理总则（讨论稿）》

10.《浙江省网络安全协调指挥平台建设指南》（2018）

11.《政务网络安全监测平台总体技术要求》TCIIA 005—2019

12.《丽水市公共数据共享安全管理规范》 （DB3311\_T 127─2020）

13.《丽水市公共数据资源管理办法》（丽政办发〔2020〕5号）

**四 技术需求**

**（一）项目背景**

2021年2月18日上午，浙江省委召开全省数字化改革大会，发布《浙江省数字化改革总体方案》，其中对政务网络安全体系提出明确要求：统筹发展网络安全与数据安全，树立网络安全底线思维，严格落实等级分级保护要求，加快建立关键信息基础设施安全保护体系、公共数据和个人信息安全保护体系，构建覆盖物理设施、网络、平台、应用、数据的网络安全技术防护体系，提升网络安全主动防御能力、监控预警能力、应急处置能力、协同治理能力，打造数字化改革网络安全屏障。

因此，加强丽水市政务网络及数据安全建设是响应浙江省数字化改革的要求，是推进丽水市数字化改革的重要举措和基础工程，项目建设将集约化、一体化、智能化贯彻始终，争做数字化改革建设排头兵。

**（二）技术需求**

* 1. **平台要求**
     1. **平台基本要求**

1. 平台采用B/S架构。
2. 平台须具备平台化的特点，重点业务模块采用独立的、模块化的设计策略，支持二次开发，平台支持主流操作系统（windows、Linux、国产化操作系统等）部署和支持主流数据库系统（MYSQL、SQLSERVER、国产化数据库等），支持国内外主流数据库和中间件，具备良好的扩展性和兼容性。支持跨平台数据传输。
3. 支持各类主流浏览器和国产化浏览器，并兼容各类主流浏览器及其不同版本。
4. 数据库设计要求。数据库需独立于应用程序，使数据库的库表结构变化不影响程序，或程序的变化也不会影响到库表结构。
   * 1. **平台安全性要求**
5. 平台中各类保密信息不会被非法窃取，具有身份验证、权限管理、细分模块访问权限。
6. 提供合理的数据备份和恢复机制，对数据库中的数据进行备份。
7. 平台设计符合信创要求。
8. 平台的安全保护等级参照三级。提供平台每年的等保三级测评，每次按照整改要求调整直至通过测评。
   1. **安全监管平台服务**

安全监管平台对接网络安全一体化支撑服务及数据安全一体化支撑服务，对政务云、网、终端、公共数据等政务信息基础设施和各类资产进行重点监测和防护，统一展示网络安全及数据安全态势感知，形成一体化对云、网络、终端、数据、应用安全监测、预警、防范、处置的闭环机制。依托大数据技术，建立安全风险感知分析能力，通过精准匹配、重点分析，提供可视化的大数据分析结果，为安全事件的研判、决策及安全重保工作提供有效支撑，加强对关键目标管控、风险识别的能力水平。同时，利用安全监管措施对安全处置流程各个阶段的安全保障工作和执行情况进行监督管理，确保安全策略在技术环节得到正确执行，相关规章制度在技术层面得到有效的支撑体现。

安全监管平台需与省级监管平台对接，按标准数据接口规范给省级监管平台上传流量、日志、资产、告警、威胁情报、安全事件等，同时接收省级平台下发的安全事件通报和风险预警。

安全监管平台还需与丽水市网信平台进行对接，实现丽水市大数据局以及其他行业监管单位、政务系统运行使用单位、信息安全支撑单位等组织在网络安全、数据安全上的协作与互通，建立健全安全监测预警、处置通报、应急处置、追踪溯源等相关机制。

安全监管平台主要分为七大模块，包括资产管理、检查督查、安全评价、处置通报、知识库管理、应急保障、可视化展示。

* + 1. **安全监管平台支撑服务**
       1. **资产管理服务**

资产管理服务通过对接浙政钉组织架构和网络安全及数据安全一体化支撑平台，获取到的单位信息和网络、数据资产信息进行统一治理后形成单位信息库。所有网络资产、数据资产均将关联到具体的单位，同时资产上存在的风险隐患、安全事件及通报预警等业务信息将通过资产管理服务自动关联到具体单位，最终形成单位画像。

* + - * 1. **服务能力要求**

1. 网络资产对接

支持通过网络安全一体化支撑平台对接，获取监管范围下的网站/系统、服务器、网络设备、安全设备、主机IP等资产，同时获取资产所属单位、负责人等相关信息。

1. 数据资产对接

支持通过数据安全一体化支撑平台对接，获取相应的数据库IP、端口，并获取元数据（库、表等信息），同时获取数据库所属单位、负责人等相关信息。

1. 单位画像

将单位下的网络资产、数据资产及资产上的相关风险、事件数据、通报预警等业务进行汇聚，通过数据自动对单位进行评判，通过不同颜色突出风险单位，帮助用户清楚掌握单位安全状况。

* + - * 1. **技术参数要求**

支持对单位库进行数据权限控制，即平台上的用户关联到具体的单位，则默认情况下该用户可查看的数据范围即为该单位所拥有的数据。

单位库中的单位应按照浙政钉规范形成相应的组织架构树，用于支撑逐层通报的接收单位智能化推荐。

* + - * 1. **服务目标要求**

通过资产管理服务摸清家底，对资产及其归属的单位进行识别。网络资产获取监管范围下的网站/系统、服务器、网络设备、安全设备、主机IP等资产；数据资产获取相应的数据库IP、端口，并获取元数据（库、表等信息）、数据库所属单位、负责人等相关信息。借助于对资产基础信息的收集及梳理，进行区域、管辖单位的匹配，形成单位画像，帮助用户了解自身或辖区内的安全风险状况。

* + - 1. **检查督查服务**

检查督查服务是丽水市大数据局定期开展检查工作的主要机制，主要包括现场检查、安全自查两个部分。通过系统管理检查工作，收集检查数据，评价检查结果。

检查督查服务包括现场检查和安全自查两种方式。

* + - * 1. **服务能力要求**

1. 现场检查

现场检查是由丽水市大数据局协同网信、公安组织技术支撑单位，制定检查计划并开展现场检查的过程。

1. 安全自查

支持各单位定期自我检查并上报检查结果。检查任务由丽水市大数据局统一设计、安排，并经过通知系统下发自查通知。

* + - * 1. **技术参数要求**

1. 现场检查

现场检查需从不同维度对工作情况进行统计说明，主要包括检查资产总数、发现的漏洞数量、年度检查的任务信息、渗透测试的情况、检查队伍评价等；

支持创建检查任务，包括任务名称、负责人、任务时间、检查对象、任务模板、支撑队伍等信息；

支持任务的基本管理，编辑、删除、查询、查看详情、提交报告、评价任务情况等。

1. 安全自查

自查统计需提供各类维度包括自查任务的数量统计、自查任务的进度情况显示、自查单位数量、自查渠道提交的漏洞数量、资产数量、测试报告数量。

支持用户自定义检查模板；

支持用户创建自查任务，并通过通知系统通知相关单位。创建自查任务可选择检查模板、填写任务目标说明、填写任务期限、选择接受单位等；

支持查看单位用户自查结果提交情况及查看任务详情；

对已提交自查结果的单位可以点击单位名称查看、下载自查结果；

需提供单位端开放自查能力，接收自查任务，自查清单，对自查任务可以下载检查模板，查看检查要求；

完成自查工作后，可以根据模板上传自查结果。

* + - * 1. **服务目标要求**

由丽水市大数据局协同网信、公安组织技术支撑单位，制定检查计划，供应商指派专业的安全服务人员进行现场检查，主要包括检查资产总数、发现的漏洞数量、年度检查的任务信息、渗透测试的情况、检查队伍评价等。同时协助丽水市大数据局进行自查统计，包括自查任务的数量统计、自查任务的进度情况显示、自查单位数量、自查渠道提交的漏洞数量、资产数量、测试报告数量。通过检查督查服务，了解本区域的安全建设情况，加强对各级单位的安全监管，提升本区域的安全防护能力，实现以查促改、以改促进。

* + - 1. **安全评价服务**

安全评价服务根据网络及数据安全检查指标库内的标准，对各类安全检查任务进行安全检查指标对比，形成统计分析和各委办、县域的安全评价，为网络安全主管部门提供数据决策支持。

* + - * 1. **服务能力要求**

1. 日常考评

为了衡量安全监管工作和整改工作的有效性，通过安全评价服务进行多项工作评价，有效促进网络安全检查工作落实，逐步提升相关单位网络安全工作水平；

安全监测工作中对被监管单位的安全监测、检查、处置过程和结果进行评价，根据被监管单位发生的中高危漏洞数量、同一安全漏洞或事件出现的频率、整改时效性、整改有效性等多项指标进行系统评价评分。

1. 管理统计

按照单位考核得分进行高低进行排名，支持考核单位所属行业及行政区域显示；支持按年切换查看历史数据；

支持日常评价统计，按照系统级别、时间对漏洞/事件趋势、最新安全事件、自检完成情况进行展示；

支持对现场检查工作情况、本发安全服务情况、本地系统建设情况等进行展示和评分；

支持数据报送统计，对技术支撑单位提供的数据量、数据质量进行综合统计，数据报送类型有资产数据、漏洞数据、事件数据、攻击威胁数据。

1. 安全评价

支持对市直单位、辖区内成员单位等网络安及数据安全状态的整体评价，支持按月、季度、半年、年度等进行安全评定。

* + - * 1. **技术参数要求**

1. 管理统计

按照单位考核得分进行高低进行排名，支持考核单位所属行业及行政区域显示；

支持按年切换查看历史数据；

支持日常考核统计，按照系统级别、时间对漏洞/事件趋势、最新安全事件、自检完成情况进行展示；

支持对现场检查工作情况、本地安全服务情况、本地系统建设情况等进行展示和评分。

1. 安全评价

支持对市直单位、辖区内成员单位等网络安及数据安全状态的整体评价；

支持按月、季度、半年、年度等进行安全评定。

添加任务列表

支持以单位为维度来跟踪各单位检查情况；

支持单个或批量开始检查任务。

信息系统基础信息管理

支持信息系统基本数据管理功能。

* + - * 1. **服务目标要求**

供应商指派专业的安全服务人员，根据网络及数据安全检查指标库内的标准，对各类安全检查任务进行安全检查指标对比，形成统计分析、安全评价和工作质量考核。安全服务人员协助丽水市大数据局开展日常考评工作，有效促进网络安全检查工作落实，逐步提升相关单位网络安全工作水平。通过安全评价服务可有效开展网络安全防护工作，了解网络安全现状，分析存在问题，通过该服务对被监管单位开展网络及数据安全工作评价，根据各类指标项评估情况等直观展示内容为监管单位提供数据决策支持。

* + - 1. **处置通报服务**

需将网络安全一体化支撑平台、数据安全一体化支撑平台监测发现的漏洞信息、安全隐患信息等推送上报到安全监管平台。

处置通报服务通过获取到的攻击、漏洞、风险、隐患等情况进行汇总，同时基于浙政钉移动端微应用提供通报处置能力。

* + - * 1. **服务能力要求**

1. 告警事件对接服务

将网络安全一体化支撑平台、数据安全一体化支撑平台监测发现的漏洞或安全隐患等通过Ka\*\*a推送或API接口对接的方式及时将情况上报到安全监管平台，经过预处理之后的安全数据以结构化的形式进行存储，对外提供数据查询与统计服务，从而实现海量数据检索与挖掘。

平台支持对安全告警的分类检索；

支持数据搜索输入框，可输入关键字包括不限于设备IP、日志发生时间、原始信息等进行检索；

支持输入时间段、表达式等条件进行检索；

支持快速选项卡检索；

可指定多个查询条件进行组合查询；

搜索结果以列表方式实现清晰展示，可在前端页面直接导出检索结果。

1. 通报预警服务

将发现到的各类中高危漏洞、数据库脆弱性等安全风险通过通报预警服务快速下发到各委办局单位及相关负责人，各局委办负责人可快速查看本单位存在的风险。当爆发重大漏洞时也可以通过预警服务对各区域、各单位进行安全预警，督促相关单位修复安全隐患，避免安全隐患成为安全事件。

1. 工单处置服务

通过工单处理服务，对发现的高危漏洞和事件，通过浙政钉微应用进行工单下发处置，处置任务的内容包括任务名称、事件描述、事件类型、事件级别、发现时间、涉及单位、单位联系人、单位联系人电话等。对下发的工单进行跟踪，负责人对工单的处理过程及结果进行记录，实现对整个工作处理过程进行跟踪，形成工单处置闭环，对逾期未处置的进行提醒。

此外，需要按照《浙政钉2.0应用上架迁移流程》将处置通报服务作为独立功能模块嵌入浙政钉，用户在浙政钉上收到告警后可直接在浙政钉上进行处置。

1. 通报方式

支持电话、浙政钉、Web端等多种通报方式。在发生严重情况如突发的安全事件、重大漏洞时，直接通过电话方式进行传达，当系统监测到存在轻微的安全隐患时可通过浙政钉等进行预警提醒或限期整改等。

* + - * 1. **技术参数要求**

1. 任务看板

支持统一的安全监管看板，在看板可以集中查看当前用户的待办通报，包括通报的事件等级、当前状态、当前进度百分比、截止时间等关键信息，支持一键联动到通报及预警信息，查看详情；

支持汇总展示当前用户收到的通报总数，通过不同标签页分别展示待处置的通报、跟踪中的通报等。

1. 安全隐患通报

支持通过浙政钉进行隐患通报指令的快速下发；

支持隐患通报的发布，发布时需填写监管接收人、单位接收人、抄送人、整改截止日期、备注等信息；

支持批量通报，可批量选择需要通报的网站进行通报；

发布成功后，可快速跳转到通报任务及时跟进整改进度。

1. 安全事件通报

支持通过浙政钉等进行事件通报指令的快速下发；

支持事件通报的发布，发布时可选择单位接收人、抄送人、处置期限、备注等信息。

1. 隐患通报跟进

支持隐患通报任务列表查看，列表字段包括网站名称、等级、行业、通报时间、整改截止日期、通报进度、通报反馈状态；

支持隐患通报进度跟进，可查看已反馈人数和未反馈人数情况；

支持隐患通报任务的筛选，筛选条件包括通报时间、反馈状态、网站名称、单位名称等信息；

支持隐患通报详情查看，包括通报状态、整改截止日期、单位接收人、抄送人等信息；

支持发布信息查看，包括发布人、发布时间、备注等信息；

支持单位信息查看，包括单位名称、所属区域、单位负责人、联系电话、单位联系人、联系电话；

支持隐患通报记录跟进记录，以时间轴的形式对发起通报、单位反馈通报处置情况等信息进行完整记录。

1. 事件通报跟进

支持事件通报任务列表查看，列表字段包括事件名称、所属区域、事件类型、通报时间、通报状态等信息；

支持事件通报进度跟进，可查看已反馈人数和未反馈人数情况；

支持事件通报任务的筛选，筛选条件包括通报时间、反馈状态、事件类型、事件名称、单位名称等信息；

支持事件通报详情查看，包括通报状态、单位接收人、抄送人等信息；

支持查看事件基本信息，信息包括事件类型、事件等级、目标IP、目标URL、所属单位、网站名称、域名、端口、发现时间、事件描述、事件截图等信息；

支持查看事件扩展信息，包括事件开始时间、事件结束时间、协议、攻击类型等信息；

支持事件通报记录跟进记录，以时间轴的形式对发起通报、单位反馈通报处置情况等信息进行完整记录。

1. 工单处理

支持将高安全风险、预警项快速的分配给具体的人员进行跟踪处理，实现责任到人，形成风险闭环。

1. 结果复审

支持相关责任单位提交隐患整改结果或事件处置结果后，并可对其反馈结果进行复核操作；

支持待复核任务的展示，展示字段包括任务名称、等级、反馈时间、通报时间、整改截止日期、通报进度、通报反馈状态；

支持待复核任务的筛选，筛选条件包括通报时间、反馈时间整改截止日期、通报反馈状态；

支持单位反馈结果查看，包括隐患整改结果、情况描述、事件处置结果、以及对应上传的附件信息；

支持对反馈结果进行复核，复核时需填写结论（通过、不通过） 、备注信息、附件信息，若复核不通过，需要责任单位重新上传反馈结果信息；

支持消息提醒，当责任单位反馈处置结果时，可实时推送单位反馈情况，及时对其进行复核操作。

* + - * 1. **服务目标要求**

供应商指派专业的安全服务人员将从网络安全一体化支撑平台、数据安全一体化支撑平台监测发现并推送上报到安全监管平台的漏洞信息、安全隐患信息等进行通报下发。通过获取到的攻击、漏洞、风险、隐患等情况进行汇总，同时基于浙政钉移动端微应用提供通报处置服务。通过处置通报服务进行告警汇总、梳理、分析，并及时通过浙政钉等方式将告警信息进行上报、通报，便于预警及快速处置，逐年提升安全事件及时处置率。

* + - 1. **知识库管理服务**

1. 知识库服务

协助丽水市大数据局建立一个安全知识库，提供各类相关标准规范文档。知识库将安全文档集中存储，统一管理，给丽水市大数据局及其他内部成员提供统一的安全学习资源的下载途径，为安全专项培训提供教材资料。

1. 事件案例服务

事件案例服务用于总结已发生的攻击事件与行为，对事件发生及处置经过进行分类梳理，形成事件案例库，为后续的网络安全工作开展提供借鉴。事件案例的产生，由发现攻击行为为起点，经过关联分析、扩线分析，产生威胁分析拓扑以及攻击画像。通过专家结合受攻击系统的等级情况，进行影响评价与定性，对于事件的处置进行跟踪记录，最后产生事件案例的最终说明。

事件案例服务将对接采集到的网络安全一体化支撑平台、数据安全一体化支撑平台等多种监测数据进行数据预处理，经过预处理后的数据存储于数据存储中心。事件来源为内生案例，同时形成案例库应用。

* + - * 1. **服务能力要求**

1. 知识库

安全知识库提供与安全相关的标准、指导性等文件，包括但不限于国家、省、市制定的各类标准制度规范、平台对接接口规范、标准解读等，便于各单位知识的学习与应用。

1. 内生案例

将安全监管平台针对告警完成的通报处置流程进行数据归档，再进行数据脱敏之后，经过分类梳理和打标、备注等过程，形成内生案例库。

内生案例库支持自动将平台上发起的所有事件通报信息进行归档展示，通过区域、事件等级、事件类型、标签、发起方、关键词对归档的预事件通报信息进行查询。同时，支持对归档的预事件通报信息进行收藏和打标，对预事件通报信息进行批注以及下载事件通报中的各类附件。

1. 案例库应用

将案例库做好数据权限划分之后，开放给各个单位，提供各单位查看的信息包括案例库中事件起因、事件发生时间、处置办法等，协助各单位更好地应对安全问题。

* + - * 1. **技术参数要求**

1. 知识库

支持建立安全知识库，包括法律法规文件、标准规范文档、接口对接规范文档、标准解读等，支持上传、下载；

支持知识库文档权限设置，可设置完全公开、仅限本部门公开。

1. 内生隐患案例入库

支持接入内部推送的重大漏洞信息并形成相应案例；

支持通过隐患名称、标题、编号、简介查询相应案例；

支持对不同类型的隐患案例进行快速搜索；

支持通过收藏按钮快速搜索本账号已收藏的隐患案例；

支持对已有的隐患案例进行编辑；

支持对已有的隐患案例进行打标和编写批注操作；

支持手动录入已有的隐患案例。

1. 内生事件案例入库

支持接入内部推送的事件信息并形成相应案例；

支持通过攻击描述、标题查询相应事件案例；

支持对不同类型的事件案例进行快速搜索；

支持通过收藏按钮快速搜索本账号已收藏的事件案例；

支持对已有的事件案例进行编辑；

支持对已有的事件案例进行打标和编写批注操作；

支持手动录入已有的事件案例。

* + - * 1. **服务目标要求**

通过知识库管理服务一方面方便各单位对标准规范、法律法规解读等知识的了解与学习，另一方面方便各单位掌握各类安全隐患及热点事件的防范及处置方法。

* + - 1. **应急保障服务**

应急保障服务用于在重要会议或重要活动期间，全方位全天候掌握与活动相关的单位、系统和网站等安全状况，高效处置安全事件。应急保障服务可实现对重保单位、技术支撑单位、安保人员、检查小组等静态数据的管理以及对安保检查、安保值守等动态业务的支撑。

* + - * 1. **服务能力要求**

1. 安保筹备

在安保筹备阶段需要对本次安保的目标对象进行安保筹备和摸底。通过安保筹备，可以让安保组织管理者和参与安保服务机构对整个安保工作的内容和范围进行整体掌握，同时对自身的安保资源如组织架构、装备工具、场地驻点和应急预案等进行全面梳理编排，并将梳理编排后的摸底成果录入系统中，便于后续通过信息化的手段对整个安保的资源和流程进行高效管理。

1. 安保检查

安保检查是支持安保组在安保期间针对重保单位开展安全检查工作，排查各类资产及系统等安全隐患。

安保检查服务包含检查统计、检查任务管理两个能力。

1. 检查统计

检查统计是针对检查任务的统计信息，可以直观查看每一轮检查任务的宏观情况，支持查看、导出每个单位、每一轮的检查结果情况。具体包括按检查单位、检查系统、漏洞隐患、任务完成情况、整改完成情况、检查人员维度来统计每一轮检查任务的检查情况。

1. 检查任务管理

检查任务管理是管理安保组的检查任务工作内容，支持安保组下发检查任务至安保检查小组，安保检查小组前往现场检查，检查完毕后出具整改通知书并将检查结果填报到平台。待单位完成整改后，安保检查小组接收单位的整改通知书并在平台上完成闭环管理。

1. 安保值守

安保值守是在安保活动进入临战阶段后日常的主要工作，安保支持服务可以对安保组在安保期间对各个驻点开展巡检工作，了解各个驻点实时安全情况，提供日历、今日排班情况和今日值守情况，便于管理人员对整体安保工作的各组工作情况进行查看和管理，同时安保值守提供的全局安保支持统览和针对具体安保活动的巡检工作管理。

* + - * 1. **技术参数要求**

1. 活动管理

支持对安保任务统一管理，包括关键字检索、新增、编辑、活动详情查看、删除、结束等操作；

支持针对重大活动建立安保任务，包括活动名称、活动时间、活动阶段（摸底阶段、备战阶段、临战阶段、决战阶段）、活动区域、活动负责人、联系方式、活动简要描述等信息。

1. 作战台

支持查看安保各个阶段的信息以及查看各个阶段的工作完成情况，工作完成与未完成采用颜色进行区分，并支持查看当前的时间所处的安保阶段；

支持将待办工作直观呈现给用户，包括通报、检查、指令、人员审批等待当前用户处理的业务流及详情查看；

支持查看与该用户有关的业务流转，实现工作跟进；

快捷方式栏支持所有业务的新增，包括新增检查任务、新增单位、新增系统、新增小组、新增人员、新增驻点、新增设备等；

直观展示用户个人的基本信息，包括所属单位。

1. 安保筹备

支持对本次安保活动的保护对象、技术支撑单位、安保人员、安保组织、驻点信息、所需设备进行统一管理，如新增、删除、编辑、查询等操作；

支持从安保人员中选择不同人员建立不同的安保小组；

支持新增、导入、编辑安保驻点，包括驻点名称、保障对象、关联人员、关联探针、驻点标签、驻点地址等；

支持按照所属单位、姓名、人员标签来进行过滤驻点关联人员；

支持对前端部署探针设备按类型及状态统计分析，对安保设备进行增、删、改、查等操作，包括设备状态等信息；

支持新建、导入、删除、下载查看应急预案，按预案等级、预案类型统计分析；

支持对安保期间的各类制度文档、应急预案等进行管理。

1. 安保检查统计

直观统计累计的检查任务数、检查单位数、检查系统数、涉及的检查人员数；

按检查单位、检查系统、检查人员三个维度直观展示每一轮检查任务的统计情况及统计每一轮检查任务的检查结果的隐患数量，以及每一轮隐患的增长趋势；

支持按检查单位、检查系统、漏洞隐患、任务完成情况、整改完成情况、检查公司、检查人员维度来统计每一轮检查任务的检查情况。

1. 检查任务

支持对检查任务进行增、删、改、查、审批等操作，检查任务详情包括检查统计、任务基本信息、检查清单、任务记录等内容；

支持在一个任务中建立多个检查小组与检查对象的检查关系；

支持现场检查和远程检查两种检查类型，远程检查时支持驻点小组上报检查的IP和提交检查结果，填写该次检查的检查结论以及检查的隐患清单；

支持审批提交的检查结果。

1. 通报统计

支持按趋势维度统计事件、隐患的趋势；

支持按事件数、隐患数、事件通报单位Top 5、隐患通报Top 5、通报进度情况等维度进行统计。

1. 安保值守

支持驻点人员报平安、报事件等业务操作；

支持在浙政钉应用上完成确定驻点各个班次的人员以及签到、签退、报平安等操作。

1. 安全事件

支持查看在活动过程中发生的待通报的安全事件，支持在详情页直接发起通报任务。

* + - * 1. **服务目标要求**

在重保期间，供应商指派专业的安全服务人员协助丽水市大数据局开展安保筹备、安保检查、检查统计、任务管理、安保值守工作，提供全生命周期的安全服务。通过应急保障服务准确把握安全威胁、风险和隐患，及时预警安全威胁情况，有效应对网络及数据安全的严峻威胁和挑战。

* + - 1. **可视化展示服务**

可视化展示服务以网络安全、云安全、数据安全以及威胁风险管理为核心，基于多维态势可视化技术，对安全相关信息进行汇聚融合，形成针对人、物、事、数据、资产的多维视图，从不同视角出发感知安全态势。

* + - * 1. **服务能力要求**

综合态势展示包含网络安全、数据安全及云安全的总体态势。总体态势主要从云、网安全角度及数据安全等角度出发。

（1）以网络安全角度出发，汇集政务信息系统的资产、威胁风险、网络攻击总体分布情况并进行综合展现。

资产态势：以资产角度出发，包括主机、安全设备等终端等不同资产类型。可实时获取当前资产总数，按区域、类型、高危资产分布。重点监控资产的可用性情况，尤其针对政务类站点进行重点实时关注，并结合地图、表单、趋势曲线图进行生动化展现。通过展示交互，还可以查看资产详细信息，包括资产所属的IP或IP段、所属系统和单位。

隐患态势：以安全威胁角度出发，包括漏洞、木马、变更、关键字、可用性等不同威胁类型。可实时获取当前安全威胁总数、各类型数量、按区域、数据来源分布、可用性分布、典型0Day、僵木蠕漏洞等获取分布信息。

攻击态势：以攻击角度出发，从攻击、访问两个维度，可实时获取当前攻击、访问总体情况，并结合地图展现攻击实况。

（2）从数据安全角度出发，数据总体风险情况分别从区域、风险类型、敏感数据使用、合规等多角度识别风险。

敏感数据分布态势：提供敏感数据类别、敏感数据分布情况、敏感数据访问、敏感数据高危告警等。

（3）从政务云安全角度出发，接收汇聚来自政务云监测发现的攻击告警数据，并通过安全监管平进行统一呈现，支持根据告警的核心字段进行检索查询，让云端安全运营管理变得更加简单，充分明晰云端资产安全情况。

（4）从安全事件角度出发，安全事件态势展示主要对安全事件进行全面的分析展现。主要从事件总体情况、事件总数、事件分类、事件处置情况、及时处置率等方面对安全事件进行整体的分析，可从中查看事件发生的规律性，对后续安全防护提供帮助。

* + - * 1. **技术参数要求**

支持资产、威胁风险、网络攻击总体分布情况，通过柱形图、饼图、趋势曲线图以及不断变化的趋势数值进行综合展现；

支持提供攻击时间、攻击源IP、目标IP、攻击类型方式、攻击路线图等环形、条形展示；

提供主要攻击类型、攻击源、被攻击目标、访问源、被访问对象分布、排行进行实时、可交互的动态展现；

支持从区域、风险类型（漏洞、攻击、API、数据库、应用等）、敏感数据使用、合规等多角度展示数据总体风险情况；

支持汇聚云租户整体数量、云资源申请数量、创建信息、部署情况、运维操作、性能监控以及销毁释放等；

支持从事件总体情况、事件总数、事件分类、事件处置情况、及时处置率等方面对安全事件进行整体的分析。

* + - * 1. **服务目标要求**

通过可视化展示服务可清晰了解本区域整体安全总体态势，方便为领导层决策时提供数据支撑，提高管理决策的科学性和精准性，提升管理效率，有效实现城市级的风险控制。

* + - 1. **对接服务**

提供对接服务，按照国家有关标准规范、结合《浙江省电子政务外网安全监测平台地市对接标准规范》等规范，完成与省级网络安全监管平台、市网信平台等对接，逐步建立安全风险报告和情报共享机制等。

服务期内，如有对接接口变更需求时则需提供二次对接开发，具体的对接要求如下：

* + - * 1. **对接省网络安全监管平台**

|  |  |  |
| --- | --- | --- |
| **序号** | **接口名称** | **接口描述** |
| 1 | 级联认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成安全监管平台至省级平台的注册功能，保证平台之间通信的安全性。由省级平台进行平台间级联的注销，省级平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 省级平台对安全监管平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 风险上报接口 | 上报频率至少为10分钟一次，含安全域名称、风险值和风险等级。 |
| 4 | 告警统计上报接口 | 安全监管平台向省级平台上报前一天发现的告警统计数据信息。含告警数量、总数、漏洞病毒高中低危告警总数等。 |
| 5 | 告警上报接口 | 安全监管平台应将本平台发现的告警信息通过告警上报接口向省级安全监测平台进行上报。含市级编码、告警时间、数据来源等。 |
| 6 | 安全事件上报 | 安全监管平台通过安全事件上报接口向省级安全监测平台进行安全事件上报。含事件等级、源目IP、文件Hash等。 |
| 7 | 案例上报接口 | 安全监管平台以文档方式进行安全事件汇总上报。含案例时间、标题、关键字、创始人、附件等。 |
| 8 | 案例知识库查询接口 | 安全监管平台可查询省级平台的知识库共享内容。含关键字、开始、结束时间等。 |
| 9 | 报表上报接口 | 安全监管平台应按要求向省级平台汇报本平台的月报报表汇总信息。含报表id、名称、类似等。 |
| 10 | 预警通报下发接口 | 省级平台定时将通报信息发送到安全监管平台中。含通报类型、描述、创建时间、附件等。 |
| 11 | 威胁情报共享接口 | 安全监管平台可向省级节点查询威胁情报信息。含行政区划码、情报IOC、IP地址、文件Hash、情报类型级别等。 |
| 12 | 漏洞上报接口 | 安全监管平台定时将漏洞信息上报到省级平台。含漏洞发布时间、级别、处置建议、参考链接等。 |
| 13 | 漏洞信息共享 | 安全监管平台可向省级节点查询漏洞信息，实现漏洞信息的共享。含关键字、开始、结束时间。 |
| 14 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，省级平台获取时需要获取文件授权（授权有时效性）再获取文件，含状态码、返回消息、存储路径等。 |

* + - * 1. **对接市网信监管平台**

|  |  |  |
| --- | --- | --- |
| **序号** | **接口名称** | **接口描述** |
| 1 | 认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成安全监管平台至网信平台的注册功能，保证平台之间通信的安全性。由网信平台进行平台间级联的注销，网信平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 网信平台对安全监管平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 工单列表信息获取接口 | 安全监管平台定时将工单列表信息上报到网信平台。含工单主题、状态、优先级、时间、受理部门、人员、创建人等。 |
| 4 | 工单详情信息获取接口 | 安全监管平台定时将工单详情信息上报到网信平台，含工单基本信息、工单详情、工单流程信息等。 |
| 5 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，网信平台获取时需要获取文件授权（授权有时效性）再获取文件。含状态码、返回消息、存储路径等。 |

* + - * 1. **对接网络安全一体化支撑平台**

|  |  |  |
| --- | --- | --- |
| **序号** | **接口名称** | **接口描述** |
| 1 | 级联认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成网络安全一体化支撑平台至安全监管平台的注册功能，保证平台之间通信的安全性。由安全监管平台进行平台间级联的注销，安全监管平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 安全监管平台对网络安全一体化支撑平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 风险上报接口 | 上报频率至少为10分钟一次，含安全域名称、风险值和风险等级。 |
| 4 | 告警统计上报接口 | 网络安全一体化支撑平台向安全监管平台上报前一天发现的告警统计数据信息。含告警数量、总数、漏洞病毒高中低危告警总数等。 |
| 5 | 告警上报接口 | 网络安全一体化支撑平台应将本平台发现的告警信息通过告警上报接口向安全监管平台进行上报。含市级编码、告警时间、数据来源等。 |
| 6 | 安全事件上报 | 网络安全一体化支撑平台通过安全事件上报接口向安全监管平台进行安全事件上报。含事件等级、源目IP、文件Hash等。 |
| 7 | 案例上报接口 | 网络安全一体化支撑平台以文档方式进行安全事件汇总上报。含案例时间、标题、关键字、创始人、附件等。 |
| 8 | 案例知识库查询接口 | 网络安全一体化支撑平台可查询安全监管平台的知识库共享内容。含关键字、开始、结束时间等。 |
| 9 | 报表上报接口 | 网络安全一体化支撑平台应按要求向安全监管平台汇报本平台的月报报表汇总信息。含报表id、名称、类似等。 |
| 10 | 预警通报下发接口 | 安全监管平台定时将通报信息发送到网络安全一体化支撑平台中。含通报类型、描述、创建时间、附件等。 |
| 11 | 威胁情报共享接口 | 网络安全一体化支撑平台可向安全监管平台查询威胁情报信息。含行政区划码、情报IOC、IP地址、文件Hash、情报类型级别等。 |
| 12 | 漏洞上报接口 | 网络安全一体化支撑平台定时将漏洞信息上报到安全监管平台。含漏洞发布时间、级别、处置建议、参考链接等。 |
| 13 | 漏洞信息共享 | 网络安全一体化支撑平台可向安全监管平台查询漏洞信息，实现漏洞信息的共享。含关键字、开始、结束时间。 |
| 14 | 资产上报接口 | 网络安全一体化支撑平台定时将资产信息上报到安全监管平台。含名称、IPv4/IPv6、MAC、责任人、操作系统、部门等。 |
| 15 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，安全监管平台获取时需要获取文件授权（授权有时效性）再获取文件，含状态码、返回消息、存储路径等。 |

* + - * 1. **对接数据安全一体化支撑平台**

|  |  |  |
| --- | --- | --- |
| **序号** | **接口名称** | **接口描述** |
| 1 | 级联认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成数据安全一体化支撑平台至安全监管平台的注册功能，保证平台之间通信的安全性。由安全监管平台进行平台间级联的注销，安全监管平台上注销后，停止与数据安全一体化支撑平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 安全监管平台对数据安全一体化支撑平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 告警事件上报接口 | 数据安全一体化支撑平台应将本平台发现的告警信息通过告警上报接口向安全监管平台进行上报。含告警类型、告警内容、告警等级、来源信息、目的信息、访问信息、告警时间、数据来源等。 |
| 4 | 数据资产上报接口 | 数据安全一体化支撑平台定时将数据资产信息上报到安全监管平台，含名称、类型、主机:端口、责任人、部门等。 |
| 5 | 元数据分级分类接口上报接口 | 数据安全一体化支撑平台定时将元数据资产信息上报到安全监管平台。含表分级分类梳理结果、列敏感识别梳理结果等。 |
| 6 | 应用服务资产上报接口 | 数据安全一体化支撑平台定时将应用服务资产信息上报到安全监管平台。含名称、主机:端口、URL、系统重要性、责任人、所属系统、部门等。 |
| 7 | API接口资产上报接口 | 数据安全一体化支撑平台定时将API接口资产信息上报到安全监管平台。含接口名称、接口地址、应用服务IP：端口等。 |
| 8 | 人员账号资产上报接口 | 数据安全一体化支撑平台定时将人员账号资产信息上报到安全监管平台。含账号名、资产、使用人、部门等。 |
| 9 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，安全监管平台获取时需要获取文件授权（授权有时效性）再获取文件，含状态码、返回消息、存储路径等。 |

* + - * 1. **浙政钉微应用**

供应商提供浙政钉微应用，需要按照《浙政钉2.0应用上架迁移流程》内置浙政钉微应用。

可通过浙政钉微应用可以展示丽水市全域的安全风险情况、事件总数、事件分类、事件处置情况、及时处置率、Top 10排名等方面，支持展示各单位总体安全得分情况、安全风险情况、处置等情况。此外，浙政钉微应用提供处置通报功能，用户在浙政钉上收到工单后可直接在内置的浙政钉微应用上进行处置。

* 1. **网络安全一体化支撑服务**

为了实现对网络安全资源的统一管理，提高安全事故发现的时效性和处理的效率，需要构建网络安全一体化支撑服务，提供对全网的网络安全事件、网络安全风险和网络安全发展态势集中监控、分析。

基于丽水市大数据局自身需求，参考《浙江省网络安全协调指挥平台建设指南（2018）》、《政务网络安全监测平台总体技术要求（TCIIA 005—2019）》，网络安全一体化支撑平台需提供数据处理分析、网络资产普查、威胁态势感知、情报关联分析分析等能力，通过对接流量采集服务、WEB应用监测服务、威胁情报数据服务、扫描评估服务、代码审计服务等具体安全服务能力，为全市政务网络提供网络安全分析和态势预测，拉通丽水市及下属各区县网络、应用、终端等各类数据，实现智能化监测，提升整体安全监管能力。

同时，本项目通过安全加固服务提升政务网络安全防护能力，包括、WiFi管控服务，非法外联检测服务。

网络安全一体化支撑服务包括网络安全一体化支撑平台服务、网络安全基础服务、网络安全加固服务三部分内容。其中，网络安全一体化支撑平台服务通过扫描监测、日志采集，流量监测、系统对接采集等技术手段，获取网络安全基础数据和动态数据，结合情报数据，纳入数据处理中心，运用分析模型进行态势分析和安全事件监测，并对分析结果进行可视化展示，对接安全监管平台将安全事件和不良态势及时向各单位和相关职能部门进行通报，并逐步实现事件溯源。

* + 1. **网络安全一体化支撑平台服务**
       1. **数据处理分析服务**

数据处理分析服务须具备多源异构安全数据采集、储存、汇聚、分析的全流程处理能力，提供网络安全监测和态势感知的支撑以及大数据存储与计算的应用支撑服务。在获取到重要网站和特定IP的远程数据、重要节点流量数据后，需及时对数据进行分析，及时发现、识别网络攻击威胁，监测恐怖组织、黑客组织、不法分子等的攻击活动、攻击行为和攻击手段；监测重点保护对象所受的攻击威胁、破坏、窃密、渗透等情况，以及重点保护对象的网络、系统、大数据等安全状况以及存在的漏洞、隐患等，对网络安全险情提供预警能力，为通报、预警、指挥等工作机制流程提供支撑。数据处理分析服务需提供多种监测数据的分析，包括重点应用监测分析、脆弱性监测分析、流量监测分析、专项安全监测分析等。

* + - * 1. **服务能力要求**

1. 需要与现有政务云、政务外网的安全系统进行对接，采集政务云安全防护及监测数据、终端安全防护数据、政务外网内目前已部署的安全设备（防火墙、IPS、IDS、防毒墙、非法外联等）的告警数据。支持定义相关告警规则，具备采集、存储、分析能力。
2. 需要实现对流量监测服务产生的数据对接。包括对市级和所有区县新建及存量的流量采集设备对接。
3. 需要实现与扫描评估服务产生的数据对接。
4. 需要实现对政务外网终端安全管理系统的数据对接。
5. 具备对WEB应用监测服务的数据进一步分析并告警的能力。
6. 具备对扫描评估服务的数据进一步分析并展示丽水政务外网的漏洞隐患情况，风险主机并排名。
7. 具备对流量监测服务的数据进一步分析并告警，具备对告警的安全事件进一步分析的能力。
8. 具备对专项安全监测的能力，如数据库服务被执行Dump操作等。
9. 具备对云、网、端、应用、数据、行为的网络安全监测能力，完成对网络安全的监测、采集、分析工作，及与安全监管平台的对接工作。
   * + - 1. **技术参数要求**
10. 支持ipv4/ipv6、多种协议的数据接入，包括但不限于FTP、SFTP、UDP、TCP、Netflow、本地文件系统、KA\*\*A、JDBC/ODBC；
11. 支持安全事件标准协议的数据；
12. 支持多文件类型的复合数据；
13. 支持动态配置模板来支持新的数据源；
14. 支持利用数据获取插件的方式利用外部通信插件式通信方式，可配置周期性调用插件主动拉取外部系统数据；
15. 支持通过前台配置的方式，实现外部数据采集；
16. 可配置外置转发器，支持单向光闸场景数据接入及不同网络间的数据采集；
17. 支持对各种来源日志进行归一化处理；
18. 支持对各种来源日志进行IP详细信息，域名详细信息，单位信息等信息的补充完善；
19. 支持对各种来源日志合并到最终统一数据流进行基础和高级分析；

⑪ 支持数据标准化处理；

⑫ 支持对相似日志的多种去重合并算法；

⑬ 支持通过正则表达式、字符串拆分等手段对原始内容进行标准化处理，支持通过配置XML文件实现快速格式定义；

⑭ 支持对数据信息进行打标签处理，以区分数据所属设备类型，支持数据打标签策略配置；

⑮ 支持针对采集日志配置数据过滤规则过滤无业务价值数据；

⑯ 支持数据采集策略的灵活配置，可配置允许接入的日志IP白名单、数据源的日志采集上限速率、来源设备IP及编码方式等，可扩展接入各类安全设备。

⑰ 支持采集数据源的界面可视化统计和监控，方便运维人员了解数据 接入的进度和状态，如可展示日志源数、已接入日志种类、接收总速率、解析速率等，并可查看接入失败的原始日志；

⑱ 支持对全库数据的复杂条件查询；

⑲ 支持对各种数据源多种维度的时间轴统计；

⑳ 支持基于平台采集的数据，利用大数据分析技术和机器学习算法，提供风险评估、风险预测服务，并持续迭代优化；

㉑ 支持将多个相分析关规则进行串联，形成链状规则增加告警的准确度；支持以图形化拖拽方式实现规则链的配置及相关参数的可视化设置；

㉒ 支持安全事件的检索能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP地址、事件类型、来源设备、威胁等级等条件进行查询， 并对查询结果提供按时间分段的统计图，查询结果以列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为Excel文件。支持在页面内展示事件详细信息，事件详情包括但不限于：事件摘要、事件关键属性，攻击过程，涉及的攻击者、受害者详情，还包括关联的日志信息、情报信息，并展示攻击者使用的ATT&CK中定义的战术及技术，以及基于攻击流程展示各项攻击技术之间的关联路径。

㉓ 支持查看平台监测的重点事件数量、疑似失陷资产（评估失陷可能性）、日志数量、攻击源数量、漏洞数量、情报数量、资产数量、设备数量、阻断事件数量等；

㉔ 支持查看安全事件的攻击区域分布，如攻击源TOP、攻击源地域TOP、事件类型TOP；

㉕ 支持安全事件分类统计和事件及隐患的排名。

㉖ 支持对接政务云部署应用和重要网站站点监测服务，支持配置安全事件同步周期、漏洞同步周期等。（支持对重要应用的漏洞、暗链、木马、攻陷检测，发布预警信息）

㉗ 支持按照时间范围、事件名称、事件类型、事件告警级别、客户端IP、载荷等查询告警信息，并支持导出。

㉘ 支持对接扫描评估服务，下发漏洞扫描任务，支持对发现的漏洞隐患进行检索查询。支持对全市政务外网和政务云的漏洞扫描。

㉙ 支持攻击溯源分析，提供安全事件攻击链查询。

㉚ 支持基于IP、URL、文件的可视化交互威胁狩猎能力，辅助安全运营人员发现未知威胁线索。包括攻击命中信息、攻击目标模型、攻击类型模型、攻击路径模型、流量命中信息，流量趋势模型、会话协议模型、端口模型、资产信息，资产开放端口、服务以及资产外联、资产被攻击事件、命中情报信息，情报命中信息及情报历史信息、同网段攻击者IP TOP推荐、IP命中的告警日志详情、恶意文件名称、恶意文件检测报告、恶意文件情报命中信息等

㉛ 支持基于全流量数据进行流量纬度的可视化统计，方方便运维人员了解流量变化情况，包括流量趋势、应用分布、主机流量、端口访问、境外访问、主机外联、域名访问、DNS请求、高频访问页面、低频访问TOP 10

㉜ 支持对存储的流量日志进行回溯查询，包括TCP/UDP会话日志、DNS解析日志、Web访问日志等，并可自定义回溯时间

㉝ 支持对原始日志的查询能力，并提供快速的全文检索条件

㉞ 支持接入还原的流量包数据，并在关联的流量日志查询页面提供下载，可作为证据上报或留存。

* + - * 1. **服务目标要求**

将政务外网现有安全产品及新增安全服务等多源异构的安全数据进行采集，通过储存、汇聚、分析，完成重点应用监测分析、脆弱性监测分析、流量监测分析、专项网络安全监测分析，实现对丽水市政务外网网络安全数据的实时分析，并输出分析结果。

**服务交付：**

* 日常时期实现5x8小时实时监测，<10分钟研判响应；若无告警，默认每2小时巡查一次威胁等级高的事件。一旦发现重大安全事件、重大漏洞隐患，将在30分钟内，通过通报预警流程通知被监测单位
* 每周、每月提供威胁分析报告
  + - 1. **网络资产普查服务**

支持通过主动探测、流量分析、人工报送、数据导入等手段汇聚网络资产数据（服务器、终端、业务应用等具备独立IP的资产）。针对核心关键资产，提供相关运营手段，自动或半自动对资产变动进行维护。同时整合资产脆弱性、关联的网络安全事件、访问情况等信息，对政务外网系统、网站、单位等关键对象进行全面画像。

* + - * 1. **服务能力要求**

1. 具备网络资产发现的能力，利用扫描评估服务或手工录入的方式发现丽水市政务外网存在的网络资产。支持按照资产拓扑的形式来对网络资产进行展示，支持对资产拓扑进行编辑的能力，并提供拓扑的预览、放大、缩小等操作。拓扑要素中包含网络资产数据（服务器、终端、业务应用等具备独立IP的资产）
2. 能对丽水政务网络的网络资产进行统一的纳管，能进一步查询编辑。
3. 能发现丽水市政务网络中的异常网络资产。
4. 具备网络资产画像的能力，能直观展现网络资产风险分布、风险类型分布、网络资产状态等。
   * + - 1. **技术参数要求**
5. 支持列表的方式统计资产信息，资产类型包括主机、网站、网段，能统计资产的基本信息、主机信息、服务信息、应用信息、所属部门和责任人登记等，且资产列表标签和资产入库规则支持自定义配置。能够统计资产的总数，以及资产分部情况。
6. 支持对发现资产形成画像，画像信息包括资产的风险分布、风险类型分布、资产状态信息。
7. 支持异常资产分析，支持自定义异常资产规则，支持对发现的异常资产进行查询分析。
8. 支持资产自动发现，能基于对接扫描评估服务、漏洞监测服务、威胁情报数据和流量数据，发现政务外网内的未知资产，能支持对发现的资产进行检索查询。
9. 支持手工录入或.xlsx文件导入资产。
10. 支持异常资产规则配置，异常资产白名单配置，可发现不合规管理的资产信息，并可展示异常资产列表和原因，便于修正资产。
    * + - 1. **服务目标要求**

通过资产自动发现、手工录入等技术手段，实现对政务外网网络资产数据（服务器、终端、业务应用等具备独立IP的资产）的统一纳管，清晰展现资产列表、资产风险、资产状态等，为资产网络安全的全生命周期管控提供基础的资产台账数据。

**服务交付：**

* 第一次存量的资产普查的时间：2个月
* 资产稽查频率：1次/月
* 每月提供资产普查报告
  + - 1. 威胁态势感知服务

威胁态势感知服务主要基于数据处理分析服务、网络资产普查服务的分析和统计结果，进行各类可视化展示。

* + - * 1. **服务能力要求**

1. 具备对政务外网网络安全威胁统一分析并展示的能力
2. 展示包括综合态势、脆弱性态势、威胁态势、运维响应态势、日志审计态势、环境感知态势等。
   * + - 1. **技术参数要求**
3. 支持多方位态势感知能力。能够进行不同层级、不同区域（包含全市）的资产态势、脆弱性态势、网络风险态势等进行评估和展示；
4. 支持主机、网站等系统的脆弱性分析展示，内容包括脆弱性资产排名、漏洞脆弱性排名、最新漏洞情报数据接入展示、系统漏洞分布、漏洞威胁分布等。支持漏洞趋势、漏洞分布趋势展示。
5. 支持网络攻击分析，内容需包含网络攻击源统计、攻击分类及统计、异常流量态势，支持多维度展示安全态势。
6. 支持运维响应态势分析，内容需包含区域通报处置总体概览、通报统计、反馈情况统计、通报处置效率统计、安全趋势等。
7. 支持对接入的日志态势分析，包括日志分类统计、日志接入统计、厂商日志统计等。
8. 支持对政务外网资产环境态势分析，包括资产风险分布、资产异常类型分布、资产设备类型统计、开放端口统计等，支持高风险资产展示，支持政务外网拓扑展示。
   * + - 1. **服务目标要求**

汇集数据处理分析服务、网络资产普查服务的分析和统计结果，通过可视化大屏进行展示，包括综合态势大屏、脆弱性态势大屏、威胁态势大屏、运维响应态势大屏、日志审计态势大屏、环境感知态势大屏，为网络安全管理者提供直观清晰的展示最新的网络安全趋势和风险状态，辅助决策安全建设方向和投资。

* + 1. **网络安全基础服务**
       1. **流量采集服务**

采集丽水市政务外网骨干网络及政务云各个节点的全流量数据，并进行多维度、全方位的威胁监测分析，提供威胁检测与态势分析的能力输出。基于大数据分析技术实现对网络流量行为的判定，发现各种层面的威胁和攻击，包括蠕虫、DDOS攻击、Web攻击等非正常和非RFC遵从的请求行为和安全事件，并能将采集的威胁告警日志上报至网络安全一体化支撑平台，供平台数据调用，从而提供事前积极预防、事中快速检测、事后溯源取证的一体化威胁监测能力，切实保障政务外网的关键业务的安全稳定运营。

* + - * 1. 服务能力要求

1. 需覆盖丽水全市电子政务外网骨干网络及政务云，采集全流量数据。
2. 能对政务外网所需要覆盖的流量进行分析。
3. 能对采集的流量进行全流量存储。
4. 在服务期内，应根据全市电子政务网络实际流量情况，对采集能力进行及时调整。
   * + - 1. **技术参数要求**
5. 流量监测服务须具备流量采集能力，能实现对网络流量元数据的采集，包括HTTP、SMTP、DNS、Telnet、TCP、UDP等多协议数据，并可以实现对其协议解析；支持对复杂多变的网络流量进行采集分析；支持流量白名单，过滤掉不关注资产流量，优化流量监测策略，提升运营效率。
6. 流量监测服务须具备威胁检测能力，具备多种功能威胁检测引擎，包括入侵检测、DoS/DDoS检测、扫描检测、Web应用检测、恶意文件检测、Webshell检测等，实现对已知威胁、威胁变种、未知威胁的快速识别分析。
7. 流量监测服务须具备流量存储能力，对应流量数据留存时长须大于7天（流量分析结果）。支持对深度解析的协议进行存储，存储日志类型至少包括：会话日志、HTTP日志、认证日志、数据库日志、DNS日志、社交账号日志等；支持对实时流量采集的PCAP包进行全量存储，支持对流量中检测到的恶意文件进行存储，供追溯分析和取证使用。
8. 支持自定义TCP端口扫描检测模型，支持配置参数包括检测阈值、检测周期，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。
9. 内置WEB应用机器学习检测模型，支持对sqli，xss，exec，phprce，ptravel和jeli攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和告警信息。
10. 支持自定义规则结合用户业务进行深度检测，自定义内容包括源IP、源端口、目的IP、目的端口、威胁级别、协议、端口和匹配特征(可匹配payload信息)。
    * + - 1. **服务目标要求**

实现对丽水市政务外网骨干网络及政务云各个节点的全流量数据采集、解析、存储、文件还原和威胁检测。发现网络流量中存在的威胁和攻击，并将事件上报至网络安全一体化支撑平台进行综合分析、研判和展示。

* + - 1. WEB**应用监测服务**

对丽水市政务外网、政务云上的WEB应用提供实时监测服务。通过监测网页挂马、网页篡改、网页敏感内容及WEB应用平稳度等多层面内容实现WEB应用完整性检测；同时还会针对这些重点应用的漏洞提供实时、高质量的漏洞监测，度量应用的风险隐患。

* + - * 1. **服务能力要求**

1. 能对政务外网、政务云上的WEB应用进行实时监测。
2. WEB应用监测服务须覆盖丽水市政务外网、政务云上的重要应用系统，服务期内日常持续监测的WEB应用数量不少于200个，重保期内根据用户需求增加相应数量。
   * + - 1. **技术参数要求**
3. 提供7\*24小时远程事件值守服务，每月一次针对重要业务的漏洞扫描及人工验证，支持对网站常见的隐患和安全灾害事故进行监测：常见隐患包括Web漏洞监测、系统漏洞监测、漏洞验证、黑链监测，常见的灾害事故包括挂马网页、篡改网页、含敏感内容网页。网站无法访问，网站域名解析异常。
4. 通过周期扫描获取当前漏洞的所处状态，根据漏洞待修复、待复验、已修复等状态的指引，做好漏洞的闭环管理
5. 至少存储备份6个月以上监测日志数据，以满足等级保护合规要求。
   * + - 1. **服务目标要求**

通过对丽水市政务外网、政务云上的WEB应用的监测。实现对这些WEB应用存在的网页挂马、网页篡改、网页敏感内容、WEB应用平稳度及漏洞隐患等问题的实时预警，帮助网络安全管理人员实时掌握网站的风险状况及安全趋势。

**服务交付：**

* 发现篡改事件、敏感内容事件、挂马事件、黒链事件、解析异常事件，漏洞隐患，将在30分钟内，通过电话、短信、邮件通知被监测单位
* 发现网站无法正常访问10分钟内，通过电话、短信、邮件通知被监测单位
* 每周、每月提供监测结果统计分析报告
  + - 1. **威胁情报数据服务**

为网络安全一体化支撑平台提供威胁情报数据，包括提供云端威胁情报数据（覆盖网络资产基础信息、指纹、漏洞库、TTP、高级威胁分析结果等不同层面）、威胁事件预警，辅助网络安全一体化支撑平台进行威胁研判。借助威胁情报数据服务，帮助用户了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握安全威胁态势，并准确地进行威胁追踪和攻击溯源。

* + - * 1. **服务能力要求**

1. 威胁情报服务能给网络安全一体化支撑平台提供威胁情报数据。
2. 威胁情报提供的数据须保证质量，情报质量需要通过以下几点进行评估：

* 网络安全一体化支撑平台威胁事件分析关联情报的事件的准确率。
* 漏洞情报预警的数量，重大漏洞的及时性及准确率。
  + - * 1. **技术参数要求**

1. 威胁情报应类型丰富、数据准确、并能够提供完整的上下文信息。可通过API查询方式，获取漏洞情报的详细信息，漏洞库数量不低于30万，更新频率至少为小时级别；威胁事件情报的详细信息，威胁事件库不低于1000条，更新频率至少为每日更新；安全舆情情报（包含特定关键字（如企业名称）的网站Title、页面信息库），更新频率至少为每日更新；IOC情报（包括远控服务器、DDoS攻击源、僵尸主机、矿池、矿机、利用漏洞攻击、利用恶意软件攻击、Web攻击、扫描源、垃圾邮件源等）；URL分类库情报，URL分类需要详细，不得少于80种，如游戏、购物、新闻等。
2. 威胁情报数据服务所使用的工具须与网络安全一体化支撑平台进行接口对接，实现情报赋能，支持平台调用自身的威胁情报数据。须承诺能与网络安全一体化支撑平台对接。
   * + - 1. **服务目标要求**

为网络安全一体化支撑平台提供威胁情报数据，辅助网络安全一体化支撑平台实现对威胁的进一步研判、威胁追踪和攻击溯源。提供最新威胁动态，帮助运营人员实施积极主动的威胁防御和快速响应策略。

* + - 1. **扫描评估服务**

要求提供扫描工具，对政务外网重要服务器、操作系统、WEB应用系统（不限于互联网网站和系统）进行持续性漏洞扫描，及时发现最新的安全漏洞，并出具详细的漏洞扫描报告及建议，配合相关单位及时对高风险漏洞进行处置。并支持将漏洞扫描数据及结果上传到网络安全一体化支撑平台对发现的安全隐患进行通报预警、跟踪处置，逐步完善漏洞全生命周期的安全体系，以及加强丽水市政务外网自身的安全水平。

* + - * 1. **服务能力要求**

扫描评估服务须覆盖丽水市网络资产普查服务中发现的所有网络资产。

* + - * 1. **技术参数要求**

1. 支持通过扫描评估服务全方位检测系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。
2. 扫描评估服务应具备行业、通用、等保的配置基线标准。通过内置基线模板的直接调用，可以快速发现偏离基线要求的配置项，节省了日常基线检查的工作量。
3. 扫描评估服务应支持云、虚拟化环境（如VMware、Hyper-v、Openstack及容器等），能够对云、虚拟化环境进行漏洞扫描以及配置核查。
4. 扫描评估服务应能够针对发现的漏洞，提供自动化漏洞验证能力，确保漏洞的真实性和降低漏洞的误报率，实现精准发现。
5. 扫描评估服务应具备行业先进性，漏洞库涵盖主流基础系统、应用系统、网络设备等系统设备，漏洞库数量应不少于21万条，并进行实时更新。同时具备丰富的配置知识库，具有多个行业的配置基线标准，可提供专业的加固修复建议。
6. 扫描评估服务的工具能提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。
7. 扫描评估服务须承诺能与网络安全一体化支撑平台对接。
   * + - 1. 服务目标要求

通过扫描评估服务，实现周期性对丽水政务外网网络资产漏洞隐患的发现，通过对漏洞隐患处置的闭环机制，实现漏洞安全全生命周期的管理。

**交付物：**

每月提供《漏洞隐患统计报告》

每月提供《漏洞处置统计报告》

* + - 1. **代码审计服务**

提供代码审计服务，完成政务外网新上线业务系统的代码审计工作，包括Java应用程序代码安全审计、C/C++应用程序（Windows、Linux、Unix平台）代码安全审计及由用户需求或监管要求引发的其他类型应用系统的代码审计。根据结果结合实际情况出具详细的审计报告及建议，并配合相关单位对不合规代码进行及时整改，降低系统的安全运行风险，满足监管和审计要求。

* + - * 1. **服务能力要求**

代码审计服务须覆盖丽水市政务外网新上线的符合等保三级及以上要求的业务系统。

* + - * 1. **技术参数要求**

1. 代码审计服务应使用代码审计工具对Java/GO/C++/Python/等源程序进行扫描，发现代码质量缺陷、安全缺陷检测、分析系统架构、应用范畴，深度查找可能存在的恶意、非法后门程序代码及安全漏洞。
2. 提供对工具的代码审计结果进行人工审查，全面分析和评估应用程序可能存在的安全缺陷，对于发现的疑似安全缺陷，根据评估情况在测试环境进行验证，同时从编码安全角度提供加固建议，从根本上修复漏洞。
3. 提供对应业务系统的《代码审计报告》作为交付物。
   * + - 1. **服务目标要求**

通过代码审计服务，实现对新上线的等保三级业务系统代码的安全审计，根据结果结合实际情况出具详细的审计报告及建议，并配合相关单位对不合规代码进行及时整改，降低系统的安全运行风险，满足监管和审计要求。

**交付物：**

对代码审计服务过的系统提供《XX系统代码审计报告》

* + 1. **网络安全加固服务**
       1. WiFi**管控服务**

提供对通过私接路由器NAT之后接入的WI-FI终端进行监管的能力，同时可支持对政务外网所有NAT环境接入的终端实现全面监管，本期建设管理终端授权并发量不低于12000个。

* + - * 1. **服务能力要求**

1. 为方便终端监管与身份识别，可支持同步浙政钉2.0组织架构。
2. 支持电脑通过浙政钉2.0 APP进行扫码登录，移动终端通过浙政钉2.0 APP实现单点登录，保证政务外网终端用户上网便捷性与使用体验。
3. 支持对监管终端分配虚拟IP，用户首次连接时分配虚拟IP，便于追溯用户访问行为。
4. 支持根据政务外网地址情况，自定义虚拟IP池和地址分配方式。
5. 支持终端以虚拟IP方式访问真实的业务系统，便于流量分析类设备进行流量分析，结合终端安全监管系统对终端安全问题进行分析和展示。
6. 支持按需授权，支持用户或用户组直接关联到应用，避免需要为部门中的个别特殊人员或用户组建立大量角色，简化权限管理。
7. 支持临时访客通过登记具有浙政钉身份的人员信息申请同等访问权限，由具有浙政钉身份人员审核账号后，开通临时账号，并设立账户有效访问时长。
8. 要求提供应急响应服务，应急处置时间在12小时之内。
   * + - 1. **技术参数要求**
9. 要求WI-FI终端监管服务提供代理网关设备支持一层或多层NAT流量穿透进行身份识别并进行结合身份权限的访问控制，提供控制中心设备对WI-FI接入移动手机终端（包含IOS9.0及以上、安卓5.0 及以上、鸿蒙全版本等主流手机操作系统）进行身份认证，并实现通扫码认证、移动手机终端通过浙政钉2.0单点登录等功能。
10. 要求支持国产电脑（飞腾芯片+银河麒麟系统V10），并承诺丽水市未适配信创终端上报后，半年内完成适配。
11. 要求代理网关设备最大理论加密流量不低于10Gbps，最大理论并发用户数不少于20000个，内存大小不低于64G，硬盘容量不低于960GB SSD，电源支持冗余电源，接口支持4千兆电口+4千兆光口SFP+4万兆光口SFP+。
12. 要求控制中心设备最大并发用户数不低于12000，内存大小不低于16G，硬盘容量不低于480G SSD，电源支持冗余电源，接口支持6千兆电口+4千兆光口+2万兆光口。
13. 支持全终端浏览器接入并访问WEB资源：
14. 支持IE8及以上版本浏览器访问WEB资源；
15. 支持Chrome 69及以上版本访问WEB资源；
16. 支持Edge、Firefox、Opera、Safari等其他主流浏览器访问WEB资源；
17. 支持微信内置浏览器、钉钉内置浏览器访问WEB资源；
18. 支持ANDROID、IOS各大手机厂商的自带浏览器访问WEB资源；
19. 支持国产操作系统浏览器接入并访问WEB资源
20. 支持全面的日志记录：
21. 支持用户登录日志（登录、注销，含MAC地址、终端类型、浏览器类型等）；
22. 支持管理员操作日志（含管理员、接入IP、时间、管理行为、对象）；
23. 支持资源访问日志（用户、源IP、URL、时间）
    * + 1. **非法外联检测服务**

提供专业的违规边界监测服务，在丽水市大数据局电子政务网范围内通过网络流量分析、主动扫描探测、数据模型分析等技术，对网络边界进行全方位实时监测,及时发现、定位非法外联、内外网互联等违规行为。监测各类设备违规边界，防止发生私自外联、业务专网直连互联网等违规行为，守住网络出口。

实现对内网中资产、网络边界、违规行为的智能感知，核心目标是全面、实时、高效地监测整个内部网络中资产状态和违规非法连接行为，并且支持实时告警、保留关键取证信息，确保内网网络的边界完整性，保障网络的物理隔离和边界防护措施到位、有效为电子政务网的安全运营提供技术保障。

* + - * 1. **服务能力要求**

**①违规互联网出口监测服务**

采用网络扫描、流量分析等技术分析发现网内存在的不合规互联网出口地址，并提供安全通报预警服务。

**②内外网互联行为监测服务**

采用网络扫描、流量分析等技术对内网直联互联网行为进行感知，发现“内外网互联”通道，利用主动发包验证技术对可疑设备进行验证，验证数据包能够到达外网告警服务器，立即对内外网互联行为进行告警，上报设备内网IP地址、互联网出口IP地址、外联时间等，并能在外联服务器上取证，并提供安全通报预警服务。

**③NAT边界监测服务**

支持自动发现管理域内的NAT设备和通过该设备私自搭建的局域网，同时上报其边界点设备IP地址、运行状态、首次发现时间、最后更新时间等信息。

**④设备资产侦测服务**

支持以交换机信息采集、主动扫描和镜像数据分析等技术手段发现网络内部的存活设备资产，并支持设备资产类型判别，包括：计算机设备、网络设备、安全设备、安防设备、办公设备、专用设备等。

* + - * 1. **技术参数要求**

提供违规边界监测服务的服务工具需满足以下要求：

1. **指标参数**

处理器≥Intel 酷睿i7

内存≥16GB（最大支持16GB\*2）

硬盘≥128GB硬盘

网络接口≥6个千兆电口，2个万兆光口

其他接口≥1个VGA接口，2个USB接口

最大镜像流量：20Gbps

最大扫描速率：50Mb/s

扫描耗时：1个B类网段平均扫描耗时约6秒

1. **内外网互联**
2. 支持不安装客户端的情况下，通过镜像流量分析和主动扫描，自动发现管理域内同时连接内网和其他网络（如：互联网）的设备。
3. 支持发现识别NAT子网内设备发起的外联行为，并可统计分析出NAT子网内可外联设备的数量。
4. 支持监测发现基于IPv6地址的外联行为。
5. 支持在外联服务器上取证，取证信息包含：外联设备内网IP、外联出口IP、发现次数、首次发现时间和最后更新时间等信息。

支持数据在外联告警系统导出。

1. **NAT接入**

支持自动发现网络管理域内的NAT设备和通过该设备私自搭建的局域网，同时上报其边界点设备IP地址、运行状态、首次发现时间、最后更新时间等信息，并能发现NAT子网中设备的IP地址等信息。

1. **资产发现**

支持以主动扫描和交换机信息采集等技术手段发现网络内部的存活资产。

1. **资产识别**

支持网络资产类型识别，包括：计算机设备（含：个人计算机、服务器、其他计算机设备等）、网络设备（含：路由器、交换机、VOIP网关、其他交换路由设备等）、安全设备（含：网闸、防火墙、入侵检测防御、VPN设备、漏洞扫描等）、安防设备（含：网络摄像机、音视频存储设备、补光灯、编解码设备等）、办公设备（含：网络打印机、办公类音视频）、专用设备（含：滤波带、电动车防盗系统、短信网关、WIFI探针、负载均衡等）。

1. **互联网告警系统**

互联网告警系统用于接收外联探测数据包，分为违规事件中转系统和违规事件展现系统。

1. **监测技术手段**

采用中心端主动扫描、镜像流量监测、网络通信嗅探等技术手段。

1. 通过中心端扫描技术手段，可对电子政务外网区的设备（包括：终端、服务器、网络设备、安全设备等）存在的违规通联行为进行监测、告警、取证，对互联网区不合规互联网出口进行监测；扫描速率最快50Mb/s，1个B类网段平均扫描耗时约6秒。
2. 通过镜像流量监测技术手段，可针对访问电子政务外网区内重要信息系统的终端设备，或与信息系统存在数据交换的服务器设备进行监测，判断来访设备是否存在与互联网通联的情况。插报间隔（5-15分钟），每间隔（5-15分钟）对配置好的镜像流量进行监测。
   1. **数据安全一体化支撑服务**

根据省大数据局《浙江省公共数据安全管理总则》要求，为不断提升、持续维持丽水公共数据安全的高质量水平，依据《数据安全能力成熟度模型（GB/T37988-2019）》标准，丽水大数据局需建设数据安全一体化支撑平台，提供对公共数据管理平台及数据仓库等数据资产的安全事件、安全风险和安全发展态势集中监控、分析，并通过对接数据资产扫描服务、数据资源清单管理服务、敏感信息识别服务、数据分类分级服务、数据安全标准映射服务等具体安全及服务能力，满足市大数据局开展数据安全统一监测、统一运行的需要。

平

提供承载丽水公共数据安全管理和技术能力的一体化支撑平台，满足国家、省、市公共数据安全工作要求，全面覆盖公共数据生命周期的各个环节，提供数据安全资源运行、数据安全策略运行、数据安全风险运行，数据安全态势感知四大综合能力，实现数据安全管理、技术防护和安全运行的有效协同。

* + 1. **数据安全一体化支撑平台服务**
       1. **数据安全一体化支撑平台服务要求**
          1. **数据安全资源运行服务**

数据资源发现服务

支持数据资源手动发现能力：手动发现是指由用户根据模板导入服务器或数据库资产信息，主要包括服务器IP地址、文件目录、数据库所属设备IP地址、数据库类型等。

支持数据资源自动发现能力:通过周期、定时任务进行端口扫描和特征发现，自动识别指定系统网段内（或指定IP地址列表端口等）存在的服务器设备列表和数据库列表，以及所分布的IP地址，并进一步探测出服务器文件系统类型、数据库类型等，数据资源类型包括不限于：MySQL、HIVE、HDFS、HBASE和Oracle。

数据资源清单服务

数据资源清单管理是数据资源管理情况的集中呈现。数据资源清单包括从外部业务系统、手工录入、数据资源扫描发现获取的数据资源。数据资源清单管理主要功能包括数据资源清单检索、数据资源认领。

数据资源清单检索：数据资源清单查询提供多种条件组合查询，查询条件至少应包含：服务器IP、资源类型、是否涉敏、所属部门、所属业务系统、责任人、对应数据、敏感数据类别、敏感数据级别等；支持数据资源列表展示，展示内容应包含：服务器IP、资源类型、是否涉敏、所属部门、所属业务系统、责任人；

支持对查询筛选后的数据资源清单进行导入，导出格式至少包含Excel；

支持数据资源清单新增、修改、删除

数据敏感识别服务

支持联动基础分级分类工具数据识别扫描能力。

可对网内各种仓储下存储的敏感信息资产进行集中任务调度管理的功能，通过持续敏感识别任务明确内部敏感数据分布。

敏感信息扫描任务管理：通过扫描任务实现仓储中敏感信息的自动发现功能，支持通过在系统中定义扫描任务对某个仓储位置的数据进行扫描，扫描方式包括立即、定期、周期等方式。

数据人工管理服务

支持管理员对敏感识别结果一键脱敏处置功能

支持人工管理的功能，允许管理员手动设定数据库/文件的结构、包含的敏感信息等。

支持可以对单个载体进行设置，也可以通过载体名称参数对具有相同结构的多个载体进行批量设置。

数据地图服务

支持通过数据地图方式对数据特性的综合进行可视化呈现。具备按照资产拓扑的形式对各个业务系统的敏感数据的分布情况进行展示的能力，拓扑呈现要素中应至少包括：业务系统名称、数据资源IP、数据分类、数据分级、特征、位置等进行呈现，并提供拓扑节点的定位、查询、放大、缩小、重置功能。

支持统计系统中接入仓储、分类分级信息分布、监视任务概况、数据监视概况、各类型包含数据标签数量分布、各敏感等级包含数据标签数量分布、仓储中各类型敏感数据分布视图。

支持对敏感数据自动识别结果及手动维护的敏感数据进行分析，生成相关报表，用户可以通此功能知道每个集群中所有数据的自动识别扫描情况，各敏感数据敏感等级的占比，各仓储中各类型敏感数据分布情况

* + - * 1. **数据安全策略运行服务**

标准管理服务

支持数据安全规范标准库的管理，实现数据安全合规项的管理，以便进行对应规范标准解读，并为数据安全策略制定提供参考依据。数据安全规范标准库包括标准检索、标准录入、标准增修、标准废止。建立数据安全事件管控策略库，提高后续相同事件处置提高效率。

策略管理服务

策略管理中包括策略的创建、变更、注销归档、下发、查询、导入及导出。由于不同类型的策略需要的字段区别较大，所以不同策略类型使用独立插件实现。在策略管理主题下按策略类型设置菜单。所有策略对象均包含以下属性：策略类型（策略类型会随着系统扩展而变化）、策略内容、状态、生效时间、失效时间、是否需要下发、已下发责任人、上次稽核时间、对应的合规项。

支持数据安全基础防护工具对接，实现对各类基础能力工具的策略下发，实现数据安全运行支撑平台的一体化运行。包含分级分类策略服务、敏感数据脱敏策略服务、水印溯源策略服务、数据加密策略服务、权限管控策略服务、多因子身份认证策略服务、出口管控策略服务数据安全策略关联服务。

事件溯源服务

支持告警内容包含用户以及ip等违规用户行为告警、数据异常、审计告警等；

支持根据IP，员工工号，为维度输出告警关联相关信息，包括：系统工号的信息，操作的频次，操作的数据相关信息安全事件输出；

支持日志存储支持非结构化数据、结构化数据、半结构化数据格式存储，支持监测日志、告警日志、应用日志、安全设备日志、主机日志等相关业务日志得存储和对外实时同步，提供安全事件溯源依据。

策略稽核服务

基于数据安全策略的稽核，实现规范标准库的落实情况跟踪、策略实际落实的情况跟踪，从而核实对规范标准的要求对应的措施的落实情况，满足规范标准库的数据安全要求。数据安全策略稽核应包括策略标准稽核、策略执行情况稽核。

* + - * 1. **数据安全风险运行服务**

安全风险定级

各安全基础能力平台上报的异常行为，通过联动分析、人工分析对异常行为进行定级。

事件处置服务

通过数据安全事件处置实现数据安全事件管理，应包括数据安全事件定级，数据安全事件处置，处置事件展示与管理，原始日志检索。

功能要求：

数据安全事件定级：数据安全事件按数据涉敏性质和量级划分事件等级，分4级：特大数据安全事件、重大数据安全事件、较大数据安全事件、一般数据安全事件，用于指导数据安全事件处置任务的紧急性和重要性。

数据安全事件处置：数据安全事件处置包括事件创建和事件处置，用户可对权限范围内的事件进行操作。

支持处置事件展示与管理：数据安全事件处置任务按状态进行分类展示，至少支持按待处置任务、历史处置任务、当前处置任务等进行展示；根据用户权限，展现用户权限范围内所有待处置任务信息，并提供操作入口。

* + - * 1. **数据安全态势感知服务**

支持包括不限于以下安全态势感知大屏：

数据共享态势大屏：展示数据对外共享流转威胁呈现

数据资源态势大屏：展示数据资源分布、涉敏、内容分类呈现

数据安全综合大屏：展示公共数据安全整体态势

* + - * 1. **一体化平台与数据安全基础能力联动服务**

一体化平台与其他数据安全基础工具进行对接，通过调用各数据安全工具的相关接口，归集安全管理相关数据并进行多维分析校核；进行数据安全策略的统一配置、下发和稽核；实现数据安全的一体化运行管理。

服务要求

支持与密码服务平台、脱敏平台、权限管控平台、多因子身份认证系统、分类分级系统、数据水印溯源系统、出口管控系统、日志审计系统对接，将各底层基础平台能力进行一体化运维。

数据安全平台需支持单点登陆、工单下发、组件API方式对接。

对接方式

单点登陆：数据安全平台支持登点至密码服务平台、脱敏平台、权限管控平台、多因子身份认证系统、分类分级系统、数据水印溯源系统、出口管控系统、日志审计系统。

工单下发：数据管控平台支持支持通过任务方式下发至密码服务平台、脱敏平台、权限管控平台、多因子身份认证系统、分类分级系统、数据水印溯源系统、出口管控系统、日志审计系统责任人，责任人登陆各安全能力执行对应安全策略。

组件API：数据管控平台支持适配分级分类组件（扫描任务、识别结果）、密码管理平台（加密应用管理）、出口管控策略（接口监测策略）、数据水印（水印策略管理）API适配。

数据采集

数据采集范围：分级分类敏感识别结果、脱敏策略执行结果、加密执行结果、数据审计（告警、日志）、出口管控（告警、日志）、数据水印执行结果。

数据采集方式：

支持包含不限于Ftp、Sftp、KA\*\*A、实时接口方式

策略下发

分级分类扫描下发：支持平台下发分级分类组件进行数据分级分类任务扫描对接

数据水印策略下发：支持平台下发数据水印标识、嵌入、分布位置等下发至水印组件

出口管控策略下发：支持平台下发接口监测（涉敏、高频）等策略至出口管控

脱敏策略：支持平台下发数据资源、脱敏结果下发至脱敏组件

加密策略：支持平台对应用加密管控的策略下发至加密组件

* + - 1. **数据安全一体化运行平台服务参数要求**

1. 确保底层数据安全基础能力平台按照设定的安全策略运行；达成数据安全全年零重大事故的目标。
2. 按月度、季度、半年度、年度出具数据安全综合报告，报告内容至少包含当前数据安全总体情况、报告期内安全事件、风险情况、整体运行情况等，并持续按照安全报告进行问题跟踪和优化提升。
3. 在服务期内完成2次《数据安全能力成熟度模型》评估，每次评估结果要有提升。
   * 1. **数据安全基础防护服务**
        1. **多因子身份认证服务**

提供多因子身份认证服务，提供桌面、移动终端访问各类业务的身份安全、统一入口、统一授权、集中接入等服务，使安全性和易用性高度平衡，提供更安全、更便捷的业务访问体验。

* + - * 1. **服务能力要求**

1. 提供动态密码生成、认证和审计的服务，将动态密码与原有账号密码认证结合，实现多因子认证保障，有效保护企业应用系统安全，同时能够帮助企业实现对访客的审计。
2. 提供APP令牌、硬件令牌、短信令牌及企业微信/钉钉H5令牌多种动态密码认证服务，支持内建/AD/LDAP等第三方账号密码认证，用户根据自身应用状况，选择合适的动态密码形式。
3. 提供双因素认证API接口服务，对接自行研发或定制开发的业务系统。同时提供数据安全管控平台与多因子身份认证对接服务，实现身份统一鉴权，有效的保护和增强数据安全管控平台的安全性。
4. 开放多因子身份认证系统接口，配合与数据安全运行支撑平台之间的对接。
5. 按照组件的方式提供服务。
   * + - 1. **服务参数要求**
6. 支持3000个用户许可接入；
7. 满足1300个手机动态令牌安装使用；
8. 支持13个应用系统的许可接入；
9. 完成一体化平台下发的安全策略配置实施。
   * + 1. **数据水印溯源服务**

通过数字水印建立数据安全标识，登记权属信息、记录交付信息、进行水印加注及鉴定，实现数据的权属证明和泄漏者溯源，不仅对数据提供方和使用方进行了确权鉴定，也对数据的泄露行为提供事后追查手段。

* + - * 1. **服务能力要求**

1. 数据接入

支持包含但不限于RDS、DRDS、PG、MAXCOMPUTE等数据库，实现按客户需求实现重点数据的数字水印接口对接。

1. 算法管理

提供对水印溯源算法管理、升级和扩展服务，支持数字、字符、不可见字符等不同方式的标识方式，两种嵌入方式（连续、间隔）及两种分布位置（固定间隔、随机间隔两种，及间隔行数自定义）的加注水印算法配置管理，方便根据场景灵活配置。

1. 标识管理

提供对数据提供方和使用方的标识码管理服务，可以单选或多选（提供方、使用方）的标识码来对数据进行动态加注。

1. 加注管理

提供对实时查询、导出的数据库数据、文件数据根据所配置的水印算法进行动态水印加注服务。

1. 溯源识别

提供对提交的可疑数据进行权属溯源服务， 对可能包含水印的部分文本数据或文件进行水印匹配溯源。达到对数据权属的确认，或数据泄露者的溯源的鉴定。

1. 水印溯源API

提供数据水印溯源API服务，通过调用开放的标准化API接口，实现对传入的数据进行水印溯源分析确权，达到对数据权属的确认，或数据泄露者的溯源。

1. 动态水印

支持动态水印，不需要落地库支持即可完成数据水印的加注；支持文件的动态水印加注。

1. 组件化

要求支持按照组件的方式提供服务。

* + - * 1. **服务参数要求**

1. 水印加注的延时在毫秒级；
2. 水印的溯源识别在秒级完成；
3. 支持分布式集群部署；
4. 支持单机并发加注水印服务的用户数在3000个以上；
5. 完成一体化平台下发的安全策略配置实施。
   * + 1. **数据日志审计服务**

通过数据日志审计服务，实现对具备各类数据库、大数据平台的全量日志采集存储，并对接入主机、安全设备、ODPS、堡垒机、各类RDS日志、结合数据流转业务流程实现日志审计与数据安全感知及预警等功能。数据日志审计服务通过采用消息队列、syslog、文件监控等技术和组件，采集大数据平台、运维、应用相关的日志，例如VPN、4A、操作系统、数据库、应用服务等，并对采集到的日志进行标准化处理，便于建模、关联等进一步分析。同时通过机器学习、数据挖掘等技术手段，自动审计分析采集到的日志，发现并感知服务器主机威胁、帐号体系威胁、用户行为威胁、数据库威胁等，出具审计报告。

* + - * 1. **服务能力要求**

数据库操作审计

提供对数据操作日志的安全审计，包括如下维度内容：

1. sql分布图：sql执行时长分布、sql响应行为分布、sql类型分布。
2. 数据抽取量分布：多维度分析各用户访问各数据库的抽取量分布图，图表展示趋势分布图，由数据项钻取显示详细列表。
3. 数据分布统计：统计数据库数量、识别敏感数据库及其数量、表数量、敏感表数量、字段数量、敏感字段数量、敏感数据类别等。
4. 数据流动统计：统计数据访问总量、敏感数据访问量、请求总量、用户数和应用数等信息。可通过直观的数据流向地图展现敏感数据的真实流转情况。

主机威胁审计

基于主机的操作日志、安全日志等内容进行分析，提供对主机威胁审计服务，包括如下维度内容：

1. 远程连接审计。监控Windows、Linux、CentOS等平台的系统主机，如主机数量、活跃情况、指令次数、密码错误次数、敏感指令次数、主机登录和远程SSH连接。
2. 异常登录审计。对于帐号的异常登录行为进行审计，包括登录时间异常、登录地点异常。
3. 异常操作审计。对用户操作行为建立行为基线，对于偏离基线的行为进行告警，包括操作时间、频率、指令类型等等。
4. 高危操作审计。对于可带来严重损害的高危操作进行感知，例如主动公网连接、特权指令执行等等。

帐号体系威胁审计

基于VPN、4A、FTP等重要系统的登录日志，对帐号体系进行威胁分析，包括如下内容：

1. 异常登录审计。对于帐号的异常登录行为进行分析，包括登录时间异常、登录地点异常。例如重点VPN帐号的境外登录等。
2. 帐号破解审计。对疑似帐号破解行为进行分析。
3. 弱口令行为审计。对于能够监测到登录过程的系统，进行口令强度分析，对弱口令进行提示告警。
4. 帐号滥用审计。对多人共享帐号的行为进行分析。

用户行为威胁审计

基于VPN、4A、主机、日志平台等重要系统的访问日志，对用户行为进行威胁审计，包括如下内容：

1. 高危指令审计。对于帐号执行高危操作进行分析，例如操作系统上的高危指令等操作。
2. 异常操作审计。从操作时间、来源、目标、频率等维度上对用户操作进行分析，确认是否偏离正常操作范围。
3. 敏感数据查询审计。对从数据库中查询敏感信息的行为进行监测，例如查询手机号、身份证号等行为。

数据库威胁审计

数据库监控要素包括主机情况、账号、实例、操作类型，支持各要素的执行排名和操作趋势展现，支持语句下钻，查看语句详请。日志详细包括源IP、数据库实例、访问账号、数据表、操作结果、操作时间等数据。另外一个维度是针对数据库资产本身的操作，即指令操作，如DDL、DML等操作，系统将指令操作与语句操作分开汇总与统计，便于数据运维人员和数据库运维人员（DBA）的管理。

1. 高危指令审计。对于帐号执行高危操作进行分析，例如数据库中清库等操作。
2. 数据库结构变化审计。对数据库表结构的变化情况进行分析，当表结构发生变化时进行提示。
3. 数据库导出审计。对从数据库中进行批量数据导出、备份行为进行安全审计。

操作回放

通过对堡垒机、linux操作日志的收集，对用户的操作行为按时间维度进行回放，回放时间内可通过时间轴进行快速跳转，并在回放过程中对高危操作进行提示。

日志采集能力：

1. 采集来源应包括服务器主机、数据库、大数据平台、文件对象存储、云桌面、堡垒机、防火墙及其它网络设备等。
2. 采集数据类型应包括账号信息、登录信息、权限信息、漏洞信息、违规信息、堡垒机日志、访问日志、管理日志、会话日志、操作日志、任务日志及异常错误日志等。
3. 采集数据项应包括但不限于协议信息、用户名、权限、登录时间、登录方式、登录来源IP、操作时间、主机名、主机类型、操作系统目录、操作指令等。

安全审计能力：

1. 具备操作指令分析能力，对相关指令进行解析，分析内容需要涵盖命令、操作、表名、文件名等，发现异常指令事件
2. 支持对数据库、应用、主机账号进行审计监控，对异常登录账号、疑似账号破解、弱口令、沉默账号、共享账号进行分析预警。

其它能力：

1. 应提供操作回放功能，在回放过程中对高危操作进行提示，并快速跳转到指定操作处
2. 应基于机器学习、数据挖掘等技术手段，自动审计分析采集到的日志，发现并感知服务器主机威胁、帐号体系威胁、用户行为威胁、数据库威胁等，并出具审计报告。
   * + - 1. **服务参数要求**
3. 支持处理不少于10个类型的日志数据，包括但不限于VPN、堡垒机、网络设备、终端agent、关系型数据库、Hdfs、Hive、Hbase、ODPS、RDS、DRDS、Petadata、GP等类型日志。
4. 日志处理性量不小于6TB/日。
5. 内置告警规则不少于100种。
6. 完成一体化平台下发的安全策略配置实施。
   * + 1. **接口管控服务**

业务系统大多基于API接口进行数据共享。针对大量的数据接口调用，需要通过出口监控能力，发现数据调用的异常情况，防止数据非法调用或泄漏。

* + - * 1. **服务能力要求**

API调用日志数据接入

支持从自动、定时获取服务接口日志，日志获取途径支持从日志系统获取或对接系统接口获取。对接公共数据平台的数据公共子平台进行接口调用日志获取。

接口管理

支持根据相关接口规范或要求，对接口进行统一规范要求，实现接口统一管理，如接口名、接口描述、输入参数、输出参数等信息的录入和管理。并针对每个接口配置相应的检测算法，一个接口对应多个检测算法。对接公共数据平台的数据共享子平台，进行接口清单获取。

接口检测

能够将日志数据与接口规则、算法进行命中分析，发现违规的数据访问。

文本检测

能够通过文档型文件审核任务，包括任务名称、数据输入路径、是否有效、检测方式，备注以及为任务选择相应检测方式。进行文档型文件检测，检测文档是否存在违规数据。

* + - * 1. 服务参数要求

1. 安全检测策略须包含不少于30种的正则表达式，须提供不少于15个程序检测算法。
2. 检测策略支持组合字段形式，可适用于对多个含义字符拼成的数据进行的检测。
3. 对文件数据安全检测的数据类型应包括手机号码、固话、身份证号、姓名、地址、邮箱等常见敏感内容检测。
4. 能承载每日检测日志量大于300G
5. 能承载每日检测日志条数大于3亿
6. 完成一体化平台下发的安全策略配置实施。
   * + 1. **数据分类分级服务**

数据分类分级服务通过对接目录系统，获取共享目录、对应元数据，并根据省大数据局发布的分类分级要求，进行评估定级。按照评估模型、评估流程对共享目录进行敏感度评估，自动识别标记敏感数据，同时，支持自定义字段敏感级别，在同步元数据时自动匹配系统库中字段敏感级别并支持人工审核修正。每季度需提供分类分级结果报告。

* + - * 1. **服务能力要求**

与公共数据平台对接

根据省大数据局发布的数据分类分级要求，结合丽水市公共数据平台情况，实现数据分类分级在公共公共数据平台的入口（用户体系对接公共数据平台）以及分类分级结果在目录系统的统一展示。提供接口对接目录系统，实现数据目录获取、目录数据展示等信息。

对接接口包括：

1. 从目录系统获取目录数据信息。
2. 向目录系统审核完成的数据的分类分级信息。
3. 提供数据分类分级信息查询服务，供各外部系统调用。

数据分类

支持对数据类别信息进行管理，可创建数据类别任务，自动对数据进行分类，并对分类的结果进行审核修正。并支持对分类分级批量任务的管理、分发、执行。

数据分级

支持按照评估模型、评估流程，对同步过来的目录数据进行敏感度评估，对数据进行定级，对目录数据自动识别标记敏感数据。

支持自定义字段敏感级别，在同步元数据时自动匹配系统库中字段敏感级别并人工审核修正。

可追溯

支持敏感数据分类分级操作日志，实现可追溯。

* + - * 1. **服务参数要求**

1. 内置分类分级知识库，包括分类分级规则库、敏感度知识库、合规知识库等类型的知识库。可自动识别数据类型至少包括个人身份相关数据、组织身份相关数据、客体相关数据、法人相关数据、经济相关数据等数据类别。
2. 数据分类分级内置规则设计一级类目有不少于5类，二级类目不少于11类，三级类目不少于88类，数据级别不少于5个。
3. 分类分级系统支持对接数据源种类不少于15种，包括但不限于mysql、oracle、Hive、HDFS、公共数据共享目录平台等多种数据源。
4. 完成公共数据平台内注册的本地个性化数据目录的分类分级；完成一体化平台下发的安全策略配置实施。
   1. **安全运行服务**

由原厂商和集成商共同组建本项目安全运行现场服务团队，在合同周期内提供驻场运行、检查评估、攻防演练、重保支撑以及安全培训等安全运行服务。

项目服务内容通过采购人组织的会议评审，并具备试运行条件后，即进入本项目的服务期，每12个月为一个服务周期。

* + 1. **驻场运行服务**

在服务期内，要求为丽水大数据局提供不少于3人的驻场服务团队，提供包括安全平台运行管理服务、平台维护服务、公共数据访问权限运行服务、共享开放接口的安全审查服务、公共数据安全审查服务、应急响应服务、协助大数据局进行制度规范提升服务、安全评价指标管理服务等。

1. 安全平台运行管理服务
2. 驻场人员定期对各平台取得的安全信息数据进行分析，以便及时发现异常行为。针对发现的可疑风险或行为，与用户技术人员进行充分沟通后，输出分析结果。
3. 针对分析结果，输出安全分析报告，在报告中提出问题处理建议、预防性维护措施等安全处理建议方法。
4. 根据各平台获取到的信息（包括但不限于漏洞及安全事件数据信息），向相关负责人汇报，汇报完成后，根据相关负责人指示授权开展进一步工作；
5. 对各平台的安全误告警进行人工研判，驻场人员与用户技术人员一起制定出相应策略，调整解决方案。
6. 在客户条件允许的情况下，对各平台的安全防护策略进行优化，保证各平台能够在最优的状态下运行。
7. 平台维护服务
8. 定期对平台进行包括功能、性能及安全策略等方面的巡检和维护。对各平台系统进行维护时，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
9. 及时提供平台功能更新服务。在合同范围内，了解并响应用户最新需求，通过快速提供升级包或在线更新跟踪等技术，在驻场运行服务过程中，提供各平台系统升级、功能更新与策略更新等服务。
10. 对各平台信息系统进行安全加固，提升操作系统安全性。在不影响数据库工作性能的前提下进行安全加固等工作；
11. 公共数据访问权限运行服务

根据丽水市公共数据中心平台的访问权限控要求，利用公共数据中心平台的数据访问权限系统提供权限新增、编辑、审核、权限越权记录核验等服务。其中授权分为客户端授权和数据授权，客户端授权用于设置哪些客户端IP可以在什么时间范围内访问目标组件；数据授权用于设置指定的目标数据载体（库、表、列、目录、文件）上可以被哪些账号执行何种操作。

1. 共享开放接口的安全审查服务

提供数据需求的安全性审查服务，提供共享开放接口的安全检查服务。包括：

1. 围绕“不落地存储数据”要求，编制各场景制度规范。
2. 完善API申请流程，增加API申请用途、分局责任人、系统建设方及责任人、存储库信息、服务进程清单等信息；与各组织、对应建设厂家责任书；
3. 通过敏感数据检测/数据规则匹配等技术手段，对数据存储环境进行定期审计和检查等。
4. 公共数据安全审查服务

建立公共数据安全的审查规范和监督检查机制，依托人工和技术手段对市本级各部门的公共数据安全提供安全审查服务。

1. 应急响应服务

为了保障应急响应的服务质量，将协助丽水市大数据局修订、完善应急预案。通过专业化服务，帮助丽水市大数据局建立健全应急响应组织以及预防、预警机制，根据应急预案规定的流程，协助丽水市大数据局进行相应的模拟演练。一旦发生紧急事件，可快速进入应急流程进行处置，保障安全监管平台信息系统的安全。

* + 1. **检查评估服务**

检查评估服务是根据国际和国内风险管理的思想，遵循国际和国内风险评估的方法论，由专业评估人员通过专业工具和分析手段，从技术和管理两个方面查找安全体系存在的漏洞和不足之处，从资产评估、脆弱性评估、安全措施有效性评估以及综合评估，最终通过全面的分析，识别出系统中当前系统所存在的风险，并在评估分析完成后提出针对性的风险控制规划措施。检查评估服务包括安全漏洞扫描、渗透测试服务、安全漏洞协助修复服务，服务期内提供不少于1次/季度的服务。

* + - 1. **渗透测试服务**

渗透测试工程师根据要求开展资产普查、信息系统上线前安全检查、渗透测试等检查，并出具渗透测试报告，以及配合相关人员进行安全加固和整改。

* + - 1. **安全漏洞协助修复服务**

在评估完成后，协助丽水市大数据局针对所发现系统的漏洞进行统一安全修复及加固，确保系统的高安全性和高可用性。

* + 1. **攻防演练服务**

服务期内，协助丽水市大数据局定期组织开展红蓝攻防演练，排摸现有网络环境可能存在的安全风险隐患，验证现有网络安全防护措施的有效性和可靠性，提供场地、平台、人员组织等服务。每年提供不少于2次的服务。

* + - 1. **攻防演练方式**

组织专业网络安全团队，由丽水市大数据局授权，针对参演委办单位提供的互联网资产，采用获取权限类、突破网络边界类、获取目标系统权限类、发现历史已有攻击事件类等攻击方式进行受控攻击。

参演委办单位组织内部网络安全专家，积极采用各类技术手段，发现各类攻击IP、攻击方式，并采取积极手段进行处置，消除安全风险并进行应急加固。同时积极尝试追踪溯源，关联分析以发现攻击源头，积极总结演练经验和报告。

最后将汇总所有参演单位进行整体演练总结。

* + - 1. **攻防演练流程**

根据相关要求，由丽水市大数据局牵头，会同重要行业部门以及信息系统责任单位，在真实网络环境下开展“背对背”实战攻防对抗。在整个演练流程过程中，丽水市大数据局将确定参演单位，在真实环境开展相关工作，演练过程中将按照“边发现，边通报，边整改”的原则，督促指导参演委办单位及时整改、消除隐患。演练结束后，将组织相关技术力量对演练进行复盘，提炼攻防技战法，形成总结报告。

* + 1. **重保支撑服务**

按照用户要求，在服务期内提供重大活动期间安全保障支撑服务（重保支撑服务）。

* + - 1. **重保时期安全检查**

在特定重保时期，驻场技术人员联合安全专家配合丽水市大数据局进行安全检查服务，将主动发现安全隐患来代替被动解决安全问题，极大的提高区域信息系统的安全防护水平。包括网络设备、主机设备、安全设备进行全面的安全巡检，如有异常情况，提供安全合规咨询建议。

* + - 1. **重保事件分析处理**

重保支撑服务完成后，安全服务人员会整理详细的重保时期业务安全报告，内容包括业务运行情况、安全事件处置情况、已造成的影响、处理办法、处理结果、预防和改进建议等内容，提交给丽水市大数据局相关人员，并根据情况划分严重级别，从而根据严重级别做出相应的服务响应。

* + 1. **安全培训服务**

服务期间开展网络安全相关培训，如：安全意识培训、安全管理培训、安全技术培训、攻防实践演练培训、应急响应实践演练培训等。使相关人员对信息安全的有初步的认识和逐步提高安全意识，让安全事故可以得到有效避免。培训内容包含网络安全法或等级保护、网络安全意识等。

* + - 1. 培训对象

根据不同的用户类型安排有针对性的培训内容。

管理人员主要包括：大数据局以及各委办局从事网络和数据安全有关工作的管理人员和技术人员。

培训目标：对管理人员的培训，目的是使他们了解国家相关部门对系统信息安全管理和建设的相关标准，同时建立起一套具有针对性和适用性的安全管理办法。

技术人员主要包括：操作人员、维护人员等。

培训目标：对技术人员的培训，目的是使他们了解信息系统所面临的严峻安全威胁和挑战，以及如何进行全面有效的安全防护措施。

* + - 1. 培训内容

1. 平台操作使用
2. 安全法规培训
3. 安全基础知识
4. 安全威胁分析
5. 安全防护措施
6. 安全管理措施
   * + 1. 培训方式
7. 现场培训：提供不少于1次/年的现场培训服务
8. 线上咨询：提供5\*8小时线上咨询服务
   * + 1. 培训地点：丽水市
   1. **安全体系保障服务**

安全是一个动态的、持续的过程。持续的安全结果与安全状态要求持续的安全过程，要求安全体系的持续稳定运行，各类安全服务以合法、合规、高质、高效的规格得到落实执行。

为保障安全体系的的持续稳健、高效地落实执行，本项目还需配套安全体系保障服务，以形成自洽的持续安全体系，具体内容包括：

* + 1. **安全制度规范服务**

依据国家相关法律法规，参考如《网络安全法》、《数据安全法》（审核稿）、《关键信息基础设施安全保护条例》（征求意见稿）、《网络安全等级保护基本要求》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《互联网信息服务管理办法》等相关法规要求及行业规范，制定覆盖数据、人员、设施、业务等四个层面的制度体系，作为安全体系建设及安全工作开展执行的依据。

本项目将建立网络安全制度规范体系和数据安全制度规范体系两大制度规范体系。

* + - 1. **安全制度规范体系**

为满足丽水市政务外网数字化建设任务的不断完善，针对标准化与体系化建设过程中涉及的业务规划、可行性研究、安全管理制度建设、合规性满足、安全运营等内容，需要配置专业咨询服务，保障相关工作告质量落实。

* + - * 1. 服务能力要求

1. 针对安全管理制度咨询，根据现状和数字化改革要求，从标准化、体系化角度，协助招标人设计整体安全建设框架，提供安全体系规划、整体安全策略、安全管理制度等咨询服务，建立健全安全管理体系。
2. 针对安全运营体系咨询，结合丽水市安全现状，制定安全运营流程和操作规范，安全事件的分类分级制度，建立健全安全运营体系。
   * + - 1. 服务参数要求

安全制度规范体系须包括：

1. 安全管理办法

按照国家及行业安全与个人用户信息保护的管理要求，如《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例》（征求意见稿）、《网络安全等级保护基本要求》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《互联网信息服务管理办法》等相关法规要求及行业规范，建立安全管理体系，制订安全管理规定,作为安全管理的顶层制度，为安全防护、运行提供依据，安全策略和标准体系的完善，为安全防护、审计、运行提供了标准依据，使安全管控有法可依，有法必依。

安全管理办法或规定的制定可通过修改、完善当前丽水局现行法规或办法等文件，并明确规范各相关方对于安全的责任和应该履行的职责、数据生命周期的安全的总体要求、安全事件通报与应急管理、安全监督与检查等相关事项的方法制定。

1. 安全管理规范

制订针对丽水市安全管理中的专项领域的管理规范和技术标准。

* 安全问责管理办法：按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，建立安全责任体系，落实安全责任，强化安全目标，保护网络及数据安全，保障各系统安全运行，提升安全防护水平。
* 安全技术标准：定义整体安全防护技术体系架构，明确安全防护通用技术要求，为丽水市政务外网及公共数据安全规划及运行提供依据。

1. 安全管理流程

针对安全管理的具体工作事项，设计安全管理流程，内容至少包括：

* 划分清楚部门管理和责任范围，明确人员角色和职责。包括数据运行部门、基础设施管理部门、业务合作部门等，统筹各部门之间的合作使用流程，履行安全合规要求。
* 明确操作流程安全注意事项，针对不同的部门、人员、业务，提供不同的操作流程。
  + - 1. **制度规范优化提升服务**

在日常运营过程中，根据相关法规更新、上级部门或监管单位检查问题、用户反馈等意见，进行综合研判分析，对当前制度中不完善的地方及时进行修改与优化，确保制度依据的先进性、合规性及合理性，确保制订的安全管理制度及规范能够稳健地承担起规范、指导丽水大数据局日常安全工作的任务。

* + 1. **安全评价指标管理服务**

安全指标管理服务关注于丽水市、县、区各部门开展网络、数据安全工作时应具备的安全能力，从组织建设、制度流程、技术工具和人员能力等四个方面，设计安全管控工作的可量化评估指标体系。通过对丽水市、县、区各部门的安全能力分级评估，生成个性化的评估报告，帮助各部门定位安全能力短板，建立安全治理体系，持续提升安全能力水平。

设计安全评价指标应包括但不限于以下范围：

1. 管理制度内容需明确包含安全管理方法、职责划分、控制文档等内容。
2. 管理制度流程需覆盖数据全生命周期流程，即采集、存储、传输、处理、交换/共享、销毁等六大流程。
3. 安全应急响应处理流程设计情况。
4. 外包人员管理及审计制度的设计。
5. 合理设计访问权限，权限设计基于三权分立架构设计。
6. 违规行为发生情况，如非法外联、非授权操作、数据违规查询、修改、删除、下载等行为。
7. 是否定期执行安全审计。
8. 安全违规事件发生情况。
9. 安全问题处理情况，包括安全缺陷整改率、安全事件改善情况等。
10. 职责人员安全能力评估情况，包括安全意识考核、技术能力考核等。

⑪ 评价指标管理，须结合大数据局实际情况定制考核指标。

* + 1. **数据全生命周期安全行为研究服务**

提供对一类典型公共数据全生命周期的分析服务，明确现有的公共数据采集、传输、存储、处理、交换、销毁等环节的实施情况，识别全生命周期中数据安全方面的风险和目前已有的数据安全防护能力，形成相应的公共数据安全实施指南，助力一体化智能化公共数据平台建设。

* + - 1. **服务能力要求**

以《浙江省数字化改革总体方案》为指导，参考《信息安全技术数据安全能力成熟度模型》、《数据安全法》等标准规范和法律法规，以不动产数据安全为例，进行不动产数据的全生命周期安全现状调研、数据安全实施指南编写等工作。

* + - 1. **技术参数要求**

服务的主要产出为报告《数据安全实施指南》，主要内容包括：

* 当前数据全生命周期实施情况；
* 数据安全风险分析；
* 当前数据安全防护能力；
* 数据安全实施指南。

**五 商务要求**

**（一）服务期**

供应商应提供三年服务，服务期起算之日为所有服务功能正式上线运行并通过采购人组织的会议评审之日。

**（二）服务要求**

1、供应商应提供至少3名专业服务人员进行5\*8小时派驻式服务，未经采购人同意，供应商不得擅自随意更换专业服务人员。驻场服务周期为项目服务周期。

驻场服务期间，驻点服务人员需通过采购人的审核方可上岗。人员具体要求由供应商根据采购人的需求针对性选择，在服务期间人员由供应商统一管理并接受采购人指挥调度。服务期间所产生的相关费用由供应商自行承担。

2、其他服务方式：

供应商需提供电话、E-Mail 和Internet 网站技术支持方式，并应建立提供专门的服务号码和账户，向用户单位提供7×24小时授权工程师电话响应服务。能够在互联网站上查询、下载相关技术资料、提交问题并获得支持。E-MAIL 最迟次日回复。

**（三）付款方式**

1.合同签订后，采购人在收到供应商开具发票之日起15日内支付第一个服务期经费的45%。

2.第一个服务期满后，根据绩效综合评价结果支付第一个服务期尾款。采购人在收到供应商开具发票之日起15日内支付该笔款项。

3.第二个服务期启动当月，采购人在收到供应商开具发票15日内支付第二个服务期经费的60%。

4.第二个服务期满后当月，根据绩效综合评价结果支付第二个服务期尾款。采购人在收到供应商开具发票15日内支付该笔款项。

5.第三个服务期启动当月，采购人在收到供应商开具发票15日内支付第三个服务期经费的60%。

6.第三个服务期满后当月，根据绩效综合评价结果支付第三个服务期尾款。采购人在收到供应商开具发票15日内支付该笔款项。

**六 安装、调试、验收要求**

**（一）供货（安装）地点要求**

根据丽水市大数据发展管理局点位布置确定。

**（二）项目人员要求**

提供服务团队组织架构、具体的人员职责分配方案、实施人员一览表、团队核心人员简历等。

**（三）项目实施计划要求**

根据项目实际情况，制定包括但不限于项目进度计划安排、项目测试计划、试运行等。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目总体进度 | 工作任务 | 1周 | 2周 | 3周 | 4周 | 5周 | 6周 | 7周 | 8周 | 9周 | 10周 |
| 项目实施准备 |  |  |  |  |  |  |  |  |  |  |
| 云资源环境部署 |  |  |  |  |  |  |  |  |  |  |
| 业务部署及测试 |  |  |  |  |  |  |  |  |  |  |
| 系统联调、开通 |  |  |  |  |  |  |  |  |  |  |
| 系统初验及试运行 |  |  |  |  |  |  |  |  |  |  |
| 项目验收 |  |  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 项目测试计划 | 确定项目 | 描述 |
| 确定测试范围 | 确定被测项目中功能模块，子功能模块等需要测试的范围。 |
| 确定测试需求 | 确定每个功能结果定义，确定此功能是否存在缺陷。 |
| 确定测试策略 | 功能测试，性能测试等。 |
| 确定测试方法 | 边界值，等价类等。 |
| 确定测试工具 | 功能测试使用Seleium，性能测试使用Jmeter等。 |
| 确定测试资源 | 测试需要的设备，服务器、参与测试的人员 |
| 确定测试交付文档 | 测试报告等 |

**（四）项目验收**

供应商应在项目实施工作结束后，向业主方提出项目验收申请，由业主方组织专家开展验收工作，并在通过验收后协助业主方完成平台的备案、日常使用的培训等相关工作，并启动持续运行维护机制。

**（五）服务绩效要求**

服务期起算之日为所有服务功能正式上线运行并通过采购人组织的会议评审之日。服务期间，需要保障服务内容和服务质量，按照丽水市大数据局统一制定的共性指标和个性评价指标进行综合考评，绩效评价打分由丽水市大数据管理局完成。具体绩效评价办法参照《丽水市大数据发展管理局信息化项目购买服务绩效评价管理细则(试行)》。

绩效评价结果采用百分制。分数权重分配：共性指标占40%；个性指标占60%，结果分为优秀、良好、一般、较差四个档次，其中：评价得分90分（含）以上为优秀、75分（含）-90分为良好、60分（含）-75分为一般、60分以下为较差。

针对每一服务期进行绩效考评，若绩效考评结果为优秀，根据合同支付尾款；绩效考评结果为良好，则要求中标供应商在1个月内对扣分项完善优化，之后根据合同支付尾款；绩效考评结果为一般，则要求中标供应商在1个月内对扣分项完善优化，之后再对其绩效复评，达到良好等级后按合同约定，扣减合同标的的5%；若绩效评价结果为较差，要求中标供应商在1个月内根据绩效考评标准对扣分项完善优化，之后再对其绩效复评，达到良好等级后按合同约定，扣减合同标的的10%；如优化后绩效考评结果仍为较差，视为不合格项目，采购人有权立即终止合同，并追究本项目的供应商违约责任。

**项目实施绩效考核指标见下表：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **指标类别** | **指标内容** | | **分值** | **评价标准** |
| 共性指标 | 进度 | | 20 | 按照服务项目合同要求完成建设。进度完成率=1-项目延期时长（月数）/合同规定服务期时长（月数）（其中延期不足一个月的部分向上取整为一个月）。  20分：各年度实施计划完成率达到90%-100%的；  10分：各年度实施计划完成率在75%（含）－90%之间的；  0分：各年度实施计划完成率在75%以下的。 |
| 质量 | | 20 | 按照服务项目合同的质量要求完成。质量达成率=1-项目中未按质量标准完成模块数/项目模块总数  20分：质量达成率为90%（含）至100%之间。  10分：质量达成率在75%（含）至90%之间。  0分：质量达成率在75%以下 |
| 范围 | | 20 | 按照服务项目合同要求完成项目内容。范围达成率=1-项目未完成模块数/项目模块总数。  20分：范围达成率为90%（含）至100%之间。  10分：范围达成率在75%（含）至90%之间。  0分：范围达成率在75%以下 |
| 资金 | | 20 | 20分：购买服务成本合理，资金使用规范；  10分：购买服务成本基本合理，资金使用较规范；  0分：购买服务成本不合理，资金使用不规范。 |
| 风险 | | 20 | 20分：购买服务过程中对风险把控适中，没有出现因风险导致的服务未完成；  10分：购买服务过程中对风险把控基本合理，没有出现因风险导致的服务未完成；  0分：购买服务过程中对风险把控不合理，出现因风险导致的服务未完成； |
| **指标类别** | **指标内容** | **分值** | | **评价标准** |
| 个性指标 | 是否出现重大安全事故 | 20 | | 服务期内，未出现重大安全事件得20分，出现一次扣10分。 |
| 安全问题及时处置率 | 10 | | 能否及时形成安全问题处置闭环；及时处置率达到70%，并逐年上升。第一个服务期的及时处置率高于70%（含），得10分。60%（含）-70%得5分。低于60%不得分；后续服务期及时处置率高于前一个服务期，得10分。60%（含）-70%得5分。低于60%不得分。 |
| 网络安全事件发现率 | 10 | | 在所有监测设备正常运转的情况下，对各级监管部门通报的网络安全事件的提前发现率(或可溯源率)，安全事件须在本次项目监测能力范围内。当总通报数量在20件及以上时，高于90%（含）得10分；80％（含）-90％得9分； 70％（含）-80％得8分；60％（含）-70％得6分；百分之60以下不得分。当总通报的数量未到达20件时，未发现一件事件扣0.5分。 |
| 数据安全成熟度模型 | 10 | | 基于当前的数据安全成熟度模型。每个服务期的成熟度模型较上一个服务期有所完善，得10分；较上个服务期无变化得5分。较上个服务期有所降低不得分。 |
| 项目信息安全和保密及纪律性 | 10 | | 遵守业主的各项管理制度和流程规范，出现项目信息安全事件、违反管理制度和流程规范等出现项目安全事故或者被相关部门通报的，出现一次扣5分。 |
| 文档质量 | 10 | | 提交的各类文档符合规范，符合通过标准，因文档质量问题影响项目进度的，扣5分并要求在3个工作日内完成整改。整改后还不符合质量要求的，该项不得分。 |
| 现场服务质量 | 10 | | 现场工作人员服务过程中，发生有理由投诉的,每次扣2分；驻场人员无故脱岗，造成业务反馈问题在15分钟后还无人响应的，每次扣2分。 |
| 项目问题响应及时率 | 10 | | 业主单位或系统使用人反馈问题后应及时响应。每发现一次问题反馈在30分钟内无响应的，扣2分，扣完为止。 |
| 项目问题处理及时率 | 10 | | 为保障系统服务质量问题处理有一定时限要求.经过问题响应分析后，应得出问题处理方案，一般问题应在2小时内解决，重大系统问题应在24小时之内解决。其中网络断网等问题不在问题范围内，但应积极配合解决问题。每发现一次，未按解决方案解决问题的，扣5分，扣完为止。因问题处理不及时造成重大社会影响的，该项不得分。 |

**七 讲解演示要求**

**（一）讲解**

1、投标人根据对项目采购需求的理解进行现场讲解，讲解内容应包含以下部分：

（1）安全监管平台服务内容讲解；

（2）网络安全一体化支撑服务内容讲解；

（3）数据安全一体化支撑服务内容讲解；

（4）安全运行服务内容讲解；

（5）安全体系保障服务内容讲解。

2、讲解时间及顺序：每个投标人讲解时间不超过15分钟，讲解顺序以政采云系统开标环节生成的顺序为准。

3、讲解方式：

（1）投标人通过政采云系统远程视频互动方式（包括直接视频互动或采用提前拍摄录制的视频）进行讲解。

（2）投标人派代表（最多不超过2人）到评审现场讲解或采用提前拍摄录制的视频方式进行讲解。

1. **演示**

1、投标人按照项目采购内容进行系统功能演示。演示内容应包含以下部分：

（1）安全监管平台服务；

（2）网络安全一体化支撑服务；

（3）数据安全一体化支撑服务。

2、演示时间及顺序：每个投标人演示时间不超过30分钟，演示顺序与讲解顺序同步进行。

3、演示方式：

（1）投标人通过政采云系统远程桌面共享方式（包括直接讲解或采用提前拍摄录制的视频）进行演示。

（2）投标人派代表（最多不超过2人）到评审现场讲解或采用提前拍摄录制的视频方式进行讲解。

**八 其他**

8.1本项目所涉及的安装数量，招标时确认数量与实际工程量不一致时，按其中标单价和实际工程量结算。税收、人工费、安装费等一切与之相关的所有费用都需包含在报价中。

8.2本项目排名第一的中标候选人未注册成为“浙江省政府采购供应商”的，采购代理机构将暂缓发布中标通知书，由此造成的不利影响自行承担。

第三章 投标人须知

投标人须知前附表（一）

| **条款号** | **条款名称** | **编列内容** |
| --- | --- | --- |
| 1.2.1 | 采购人 | 见第一章招标公告（邀请） |
| 1.2.2 | 采购代理机构 | 见第一章招标公告（邀请） |
| 1.4.1 | 联合体投标 | ☑ 不接受；  □ 接受。 |
| 1.7.1 | 现场踏勘 | ☑ 不组织。  □ 组织，详见第二章招标需求。 |
| 1.8.1 | 答疑会 | ☑ 不召开；  □ 召开。时间： 年 月 日 时 分；地点： |
| 1.9.1 | 分包 | ☑ 1.不允许。  □ 2.允许，但主体部分不得分包，详见第二章招标需求 |
| 1.11.1 | 小型、微型企业的价格扣除 | 1. 对小型和微型企业产品给予6%的价格扣除；  2. 联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%，给予XX%的价格扣除；  3. 本项目所属行业：软件和信息技术服务业；  4. 专门面向中小企业的项目，不享受价格扣除。 |
| 1.13.6 | 质疑联系人 | 1. 采购需求、供应商资格条件及评审办法质疑：  单 位：丽水市大数据发展管理局  联系人：朱坚 联系电话：0578-2091985 传真：/  2. 其他事项质疑：  单 位：丽水市公共资源交易中心  联系人：刘晓华 联系电话：0578-2292511 传真：0578-2292507 |
| 1.13.11 | 同级政府采购监督管理部门 | 见第一章招标公告（邀请） |
| 2.2.4 | 澄清、修改发布网址 | 1. 浙江政府采购网（[zfcg.czt.zj.gov.cn](http://www.zjzfcg.gov.cn)）  2. 丽水市公共资源交易网（lssggzy.lishui.gov.cn） |
| 3.4 | 资格审查文件组成 | ▲1. 有效的营业执照电子文档；  ▲2. 负责人身份证电子文档。  ▲3. 若有委托代理人的，则还应当提供授权委托书及委托代理人的身份证电子文档；  ▲4. 具有良好的财务会计制度、依法缴纳税收和社会保障资金的承诺函；  ▲5. 具有履行合同所必需设备和专业技术能力的承诺函；  ▲6. 无重大违法记录声明书；  ▲7. 联合体协议书（若有）；  ▲8. 特定资格条件证明材料电子文档（若有）；  9. 其他。  注：编制格式要求见第五章投标文件格式，无格式的自行设计。 |
| 3.5 | 资信商务及技术文件组成 | 1. 投标函；  2. 投标人资质  3. 成功案例及业绩  4. 服务需求理解分析  5. 服务能力  6. 安全监管平台服务方案  7. 网络安全一体化支撑平台服务  8. 网络安全基础服务  9. 网络安全加固服务  10. 数据安全一体化支撑平台服务  11. 数据安全基础防护服务  12. 安全运行服务  13. 安全体系保障服务  14. 拟投入的项目团队履历及能力要求  15. 投标人需要说明的其他文件和证明。  注：编制格式要求见第五章投标文件格式，无格式的自行设计。 |
| 3.6 | 报价文件组成 | 1. 开标一览表；  2. 投标分项报价表；  3. 中小企业声明函（若有）；  4. 监狱企业声明函（若有）；  5. 残疾人福利性企业声明函（若有）。  注：编制格式要求见第五章投标文件格式，无格式的自行设计。 |
| 4.3.1 | 投标有效期 | 90 天 |
| 4.5.1 | 投标文件份数 | **1. 电子加密投标文件：政府采购云平台在线提交、上传一份；**  **2. 备份投标文件：电子邮件提交一份，由投标人自行确定是否提交；若提交请将备份投标文件以电子邮件的形式发送至（lssggzyjyzx@163.com）。**  **注：投标人在线解密失败后，启用备份投标文件，否则不启用备份投标文件。** |
| 6.1.1 | 开标时间和地点 | 见第一章招标公告（邀请），**投标人可以远程在线参加，不必现场参加开标** |
| 6.3.1 | 评标方法 | ☑ 综合评分法  □ 最低评标价法 |
| 8.2.1 | 中标公告发布网址 | 1. 浙江政府采购网（[zfcg.czt.](http://zfcg.czt.zj.gov.cn/)[zj.gov.cn](http://zfcg.czt.zj.gov.cn/)）  2. 丽水市公共资源交易网（[lssggzy.lishui.gov.cn](http://www.lssggzy.com)） |
| 8.3.1 | 履约保证金 | 无 |

投标人须知前附表（二）

**招标活动日程安排表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 时间安排 | 备注 |
| 1 | 发布招标公告 | 2021年9月3日 | 1.浙江政府采购网（[zfcg.czt.zj.gov.cn](http://www.zjzfcg.gov.cn)）  2.丽水市公共资源交易网（[lssggzy.lishui.gov.cn](http://www.lssggzy.com/)） |
| 2 | 发放招标文件 | 2021年9月3日起 | 获取方式：招标公告附件自行下载 |
| 3 | 现场踏勘和地点 | ☑ 无  □ XXXX年XX月XX日XX时，  地点： |  |
| 4 | 更正公告 | 澄清或修改内容可能影响投标文件编制的，提交投标文件截止时间15日前，不足15日的，顺延提交投标文件截止时间； | 澄清或修改内容获取方式：更正公告 |
| 5 | 提交投标文件截止时间 | 见第一章招标公告（邀请） |  |
| 6 | 开标时间 | 见第一章招标公告（邀请） |  |
| 7 | 中标公告及中标通知书 | 中标人确定之日起2个工作日内 |  |
| 8 | 质疑期限 | 中标结果公告期限届满之日起7个工作日内 |  |
| 9 | 投诉期限 | 质疑答复期满后15个工作日内 |  |
| 10 | 签订合同 | 中标通知书发出之日起30日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。 |  |

一 总则

1.1 适用范围

招标文件适用于本次招标项目的采购行为，法律、法规另有规定的，从其规定。

1.2 定义

1.2.1 “采购人”是指：见投标人须知前附表（一）；

1.2.2 “采购代理机构”系指招标公告中载明的本项目的采购代理机构，详见投标人须知前附表（一）；

1.2.3 “投标人”系指按照本招标文件的规定参加并递交投标文件的自然人、法人或其他组织；

1.2.4 “负责人”系指法人企业的法定代表人，或其他组织为法律、行政法规规定代表单位行使职权的主要负责人，或自然人本人；

1.2.5 “投标人代表”系指负责人或其授权的委托代理人；

1.2.6 “合同”系指采购人与中标人双方签署的规定双方权利与义务的协议，以及所有附件、附录、招标文件和投标文件所提到的构成合同的所有文件；

1.2.7 “服务”系指投标人按招标文件规定应承担的服务内容，包括送货上门、安装、调试、技术协助、维修、产品三包制度、校准、培训、技术指导以及其他类似的附随义务；

1.2.8 “产品”系指投标人按招标文件规定，须向采购人提供的一切产品（包括：虚拟产品），以及产品相关的保险、税金、备品备件、附件、耗材、工具、手册及其它有关技术资料和材料等；

1.2.9 “项目”系指投标人按招标文件规定向采购人提供的服务和产品；

1.2.10 标有“▲”符号均属于“实质性条款”，不允许负偏离；

1.2.11 标有“★”系指项目关键核心产品，作为判断同品牌产品的依据。

**1.2.12 “电子投标文件”系指投标人通过“政采云电子交易客户端”编制的数据电文形式的“电子加密投标文件”。**

**1.2.13 “备份投标文件”系指与“电子投标文件”同时生成的数据电文形式的电子文件。**

1.3 投标人应具备资格条件

1.3.1 符合本文件第一章“第二条”的规定；

1.4 联合体

1.4.1 联合体：见投标人须知前附表（一）；

1.4.2 联合体各方均符合政府采购法第二十二条第一款规定；

1.4.3 联合体中至少有一方符合本文件规定的特定资质要求。但联合体中有同类资质的投标人按照联合体分工承担相同工作的，应当按照资质等级较低的投标人确定资质等级；

1.4.4 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他投标人另外组成联合体参加同一合同项下的政府采购活动；

1.4.5 联合体参与的，必须提供《联合体协议书》。

1.5 投标文件的语言及计量

1.5.1 投标文件以及投标人、采购人与采购代理机构就有关投标事宜的所有来往函电，均应以简体中文书写，除签名、盖章、专用名称等特殊情形外；

1.5.2 投标资料提供外文证书或者外国语视听资料的，应当附有中文译本，由翻译机构盖章或者翻译人员签名；

1.5.3 投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应当采用中华人民共和国法定计量单位。

1.6 投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用。

1.7 现场踏勘

1.7.1 采购人或采购代理机构按投标人须知前附表（一）规定的时间、地点组织投标人现场踏勘；

1.7.2 投标人踏勘现场发生的费用自理；

1.7.3 除招标人的原因外，投标人自行负责在踏勘现场中所发生的人员伤亡和财产损失；

1.7.4 招标人在现场踏勘中介绍的场地和相关的周边环境情况，供投标人在编制投标文件时参考，采购人不对投标人据此作出的判断和决策负责；

1.7.5 投标人自身原因不参与现场踏勘的，不得就此提出质疑。

1.8 答疑会

1.8.1 采购人或采购代理机构按投标人须知前附表（一）规定的时间和地点召开答疑会；

1.8.2 答疑会后，采购人或采购代理机构按本章第2.2款规定对投标人所提问题进行澄清答复；

1.8.3 投标人自身原因不参与答疑会的，不得就此提出质疑。

1.9 分包

1.9.1 分包：见投标人须知前附表（一）；

1.9.2 投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

1.10 保密

参与招标投标活动的各方当事人应当对评标情况以及在评标过程中的获悉的国家秘密、商业秘密负有保密责任，违者应对由此造成的后果承担法律责任。

1.11 政府采购政策

1.11.1 根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）文件要求，在政府采购活动按下列情形之一给予价格扣除：

⑴对于非专门面向中小企业的项目，对小型和微型企业产品的价格给予扣除，用扣除后的价格参与评审，价格扣除比例见投标人须知前附表（一）；

⑵大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，可给予价格扣除，用扣除后的价格参与评审。联合体各方均为小型、微型企业的，联合体视同为小型、微型企业。价格扣除比例见投标人须知前附表（一）；

⑶参加政府采购活动的中小企业应当提供《中小企业声明函》。

1.11.2 投标人符合《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）文件要求，并提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，则视同小型、微型企业，享受第1.11.1条的扶持政策；

1.11.3 投标人符合《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）文件要求，并提供《残疾人福利性单位声明函》的，则视同小型、微型企业，享受第1.11.1条的扶持政策。

1.11.4 ▲采购进口产品：招标需求中未注明进口产品或允许进口产品，不得提供进口产品。

1.12 信用信息记录查询

1.12.1 查询渠道：信用中国网站（[www.creditchina.gov.cn](https://www.creditchina.gov.cn/)）、中国政府采购网（[www.ccgp.gov.cn](http://www.ccgp.gov.cn)）；

1.12.2 信用信息记录查询截止时间：同资格审查结束时间，网站显示的信用信息记录将作为投标人资格审查的依据；

1.12.3 查询内容：列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

1.12.4 信用信息留存方式：信用信息查询记录和证据以网页页面打印（或截图）等方式进行留存；

1.12.5 联合体成员存在不良信用信息记录的，视同联合体存在不良信用记录。

1.13 质疑和投诉

1.13.1 投标人认为招标文件、招标过程、中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑。

1.13.2 提出质疑的投标人应当是参与所质疑项目招标活动的投标人；

潜在投标人已依法获取其可质疑的招标文件的，可以对该文件提出质疑。对招标文件提出质疑的，应当在获取招标文件或者招标文件公告期限届满之日起7个工作日内提出；

1.13.3 同一招标程序环节的质疑，投标人须一次性提出，否则不予以答复；

1.13.4 质疑主要内容应符合《政府采购质疑和投诉办法》（财政部94号令）等相关规定，质疑内容涉及保密事项，质疑人应提供有效的信息来源或有效证据；

1.13.5 质疑人可直接提交、传真或邮寄方式提交质疑函（一式三份以上）。以其他方式提出的质疑，采购人或采购代理机构可不予接受、答复。

⑴邮寄方式送达质疑函的，以采购人或采购代理机构实际收到邮件之日作为收到质疑的日期。

⑵传真方式送达质疑函的，质疑人应当取得采购人或采购代理机构确认收到传真的意见，并及时将质疑函原件送达采购人或采购代理机构。采购人或采购代理机构以实际收到原件之日作为收到质疑的日期。

⑶在质疑期限届满前，质疑函已经邮寄或传真成功的，质疑不视为过期。

1.13.6 质疑联系人：见投标人须知前附表（一）

1.13.7 相关当事人提供外文证书或者外国语视听资料的，应当附有中文译本，由翻译机构盖章或者翻译人员签名。相关当事人向财政部门提供的在中华人民共和国领域外形成的证据，应当说明来源，经所在国公证机关证明，并经中华人民共和国驻该国使领馆认证，或者履行中华人民共和国与证据所在国订立的有关条约中规定的证明手续。相关当事人提供的在香港特别行政区、澳门特别行政区和台湾地区内形成的证据，应当履行相关的证明手续；

1.13.8 采购人或采购代理机构在收到质疑人的书面质疑后7个工作日内作出答复，并以书面形式答复质疑人；

1.13.9 质疑人捏造事实、提供虚假材料进行质疑的，采购人或采购代理机构报告同级政府采购监督管理部门，由同级政府采购监督管理部门审查，情况属实的，应列入不良行为记录，并在指定的媒体上公告；

1.13.10 质疑人对采购人或采购代理机构的答复不满意或者采购人、采购代理机构未在规定时间内答复的，可以在答复期满后15个工作日内向同级政府采购监督管理部门提起投诉；

1.13.11 同级政府采购监督管理部门：见投标人须知前附表（一）

1.13.12 质疑函、投诉书范本在浙江政府采购网（zfcg.czt.zj.gov.cn）-下载专区中下载。

1.14 特别声明

1.14.1 ▲单位负责人为同一人或者存在直接控股、管理关系的不同投标人，以及属于同一母公司或集团的不同投标人不得参加同一合同项下的政府采购活动；

1.14.2 ▲为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动；

二 招标文件

2.1 招标文件的组成

2.1.1 第一章 招标公告（邀请）；

2.1.2 第二章 招标需求；

2.1.3 第三章 投标人须知；

2.1.4 第四章 政府采购合同格式；

2.1.5 第五章 投标文件格式；

2.1.6 第六章 评标办法及标准；

2.1.7 本项目招标文件的澄清、修改的内容。

2.2 招标文件的澄清、修改

2.2.1 投标人应仔细阅读和检查招标文件的全部内容。发现其中有误或有不合理要求的，应当在招标文件的澄清、修改截止时间前以书面形式要求采购人或采购代理机构对招标文件予以澄清、修改；

2.2.2 澄清或修改内容可能影响投标文件编制的，采购代理机构在提交投标文件截止时间15日前，将以发布更正公告的形式通知各潜在的投标人。不足15日的，采购代理机构有权顺延提交投标文件截止时间；

2.2.3 提交投标文件截止时间前，采购代理机构可以对发出的招标文件进行必要的澄清或修改，澄清或修改后的补充文件，作为招标文件的组成部分，对各投标人起同等约束作用；

2.2.4 澄清、修改等更正内容发布网址：见投标人须知前附表（一）；

2.2.5 当招标文件与澄清或修改文件就同一内容的表述不一致时，以最后发出的澄清或修改文件为准。

三 投标文件

3.1  投标文件的形式和效力

3.1.1 投标文件形式：电子投标文件（包括“电子加密投标文件”和“备份投标文件”，“电子加密投标文件”和“备份投标文件”在投标文件编制完成后同时生成）。

3.1.2 投标文件的效力：“电子加密投标文件”和“备份投标文件”具有同等效力，数据电文内容应完全一致。

3.1.3 ▲电子加密投标文件按时解密成功的，备份投标文件自动失效；电子加密投标文件解密失败，按招标文件规定提交备份投标文件且有效的，以备份投标文件为准；电子加密投标文件解密失败，又未提交备份投标文件，视同放弃投标。

3.2 在线投标响应（电子投标）说明

3.2.1 本项目通过政府采购云平台实行电子投标，应按照本项目招标文件和政府采购云平台的要求编制；投标人在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政府采购云平台技术支持热线咨询，联系方式：400-881-7190。

3.2.2 标前准备：各投标人应在开标前确保成为浙江省政府采购网正式注册入库供应商，并完成CA数字证书办理（办理流程详见电子投标工具链接：[http：//zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12945.html](http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12945.html)）。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由投标人自行承担。

3.2.3 投标文件制作：投标人通过政府采购云平台电子投标工具制作投标文件，电子投标工具请投标人自行前往浙江省政府采购网下载并安装（下载网址：http：//[zfcg.czt.zj.gov.cn/bidClientTemplate/2019-09-24/12975.html](http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-09-24/12975.html/)），电子投标具体流程文档详见网址：[https：//service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na](https://service.zcygov.cn/" \l "/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na)。

3.2.4 本项目通过政府采购云平台进行开标、资格审查、评审、询标，投标人均应当准时在线参加，否则产生的风险由投标人自行承担（投标人务必不要离开电脑太久，并留意手机短信，建议投标人提前做好检查“政府采购云平台”内，关于“项目采购”的岗位权限是否勾选。如有问题，请致电400-881-7190）。

3.3 投标文件组成

投标文件由【资格审查文件】、【资信商务及技术文件】、【报价文件】三部分组成。

3.4 资格审查文件的组成

资格审查文件的组成：见投标人须知前附表（一）。

3.5 资信商务及技术文件的组成

资信商务及技术文件的组成：见投标人须知前附表（一）。

3.6 报价文件的组成

报价文件的组成：见投标人须知前附表（一）。

四 投标文件的编制

4.1 投标文件编制

4.1.1 ▲本招标文件中若有多标项的，若参与多标项投标的，则按每个标项分别独立编制投标文件；

4.1.2 电子投标文件编制请按政府采购云平台供应商项目采购-电子招投标操作指南（网址：[https：//service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na](https://service.zcygov.cn/" \l "/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na)）和本招标文件要求编制并进行关联定位。

4.1.3 投标人应按招标文件的要求提供相关资料，并对招标文件中提出的所有内容要求给予明确响应，须保证投标文件的准确、真实、明确。投标文件响应内容对招标文件要求如有偏离均应填写偏离表，如不填写，评标委员会有权视作投标文件不完全响应招标文件要求；

4.1.4 投标文件编制时应有正确的索引目录及连续页码标注；

4.1.5 投标文件须清晰可辨，因模糊不清所引起的后果由投标人自行负责。

4.2 投标报价要求

4.2.1 ▲投标报价是履行合同的最终价格，包括服务内容、包装、工时、运输、装卸、保险、税金、安装、调试与试运行、培训、保修、售后服务费、配套费、以及实施本项目所需的其他一切费用；

4.2.2 ▲投标文件只允许有一个报价，有选择的或有条件的报价将不予接受。

4.3 投标有效期

4.3.1 ▲投标有效期：见投标人须知前附表（一）。投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期；

4.3.2 在特殊情况下，采购人可与投标人协商延长投标书的有效期，这种要求和答复均以书面形式进行。

4.4 投标文件格式

投标文件格式见招标文件“第五章投标文件格式”，投标文件应当按照招标文件已提供的格式填写，无格式的可自行设计。

4.5 投标文件份数及签署

4.5.1 ▲投标文件份数：见投标人须知前附表（一）；

4.5.2 投标文件中所须加盖公章部分均采用CA签章。

五 投标文件的提交

5.1 投标文件导入和加密

5.1.1 投标人应当按照资格审查文件、资信商务及技术文件和报价文件三部分分别导入相应位置，各文件之间不得导错位置；

5.1.2 投标文件编制好后应当生成电子加密投标文件，生成电子加密投标文件具体操作详见（电子招投标操作指南网址：[https：//service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ](https://service.zcygov.cn/" \l "/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na)[8Na](https://service.zcygov.cn/" \l "/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na)）。

5.2 投标文件的提交

5.2.1 提交投标文件截止时间：见第一章招标公告（邀请）

5.2.2 提交投标文件地点：见第一章招标公告（邀请）

5.2.3 不予接收的投标文件情形

▲⑴提交投标文件截止时间前未完成传输的投标文件；

▲⑵未生成加密的投标文件；

5.2.4 投标人所提交的投标文件不予退还。

5.3 投标文件修改和撤回

5.3.1 在提交投标文件截止时间前，投标人可对已提交的投标文件进行补充、修改或撤回。补充、修改投标文件的，应当先行撤回原文件，补充、修改后重新生成加密的投标文件并重新上传提交；

5.3.2 补充、修改后重新提交的投标文件应按招标文件的规定编制、加密、导入和提交；

5.3.3 在提交投标文件截止时间后，投标人不得修改、撤回已提交的投标文件。

5.4 备选投标方案

本项目不接受备选投标方案。与“电子投标文件”同时生成的“备份投标文件”不是投标备选（替代）投标方案。

**5.5 投标诚实信用**

5.5.1 投标人应当遵守诚实信用原则。

5.5.2 投标人有下列情形之一的，将会报告财政部门并按照相关规定处理：

⑴投标人在投标有效期内撤销投标文件的；

⑵未按规定提交履约保证金的；

⑶投标人在投标过程中弄虚作假，提供虚假材料的；

⑷中标人无正当理由不与采购人签订合同的；

⑸投标人有串通投标行为的；

⑹严重扰乱政府采购程序的；

⑺违反其他法律法规规定的情形。

5.5.3 因投标人有第5.5.2条情形之一造成采购人和采购代理机构损失的，采购人和采购代理机构有权追究投标人赔偿责任。

六 开标和评标

**本项目通过政府采购云平台进行开标、资格审查、评审、询标，投标人应当准时在线参加，否则产生的风险由投标人自行承担（投标人务必不要离开电脑太久，并留意手机短信，建议投标人提前做好检查“政府采购云平台”内，关于“项目采购”的岗位权限是否勾选。如有问题，请致电400-881-7190）。**

6.1 开标

6.1.1 开标时间和地点：见投标人须知前附表（一）

6.1.2 投标人的投标人代表应当在线参加，否则视同认可开标结果，事后不得对采购相关人员、开标过程和开标结果提出质疑；

6.1.3 开标程序

⑴主持人宣布项目开标会开始，介绍参加本次开标会的相关人员；

⑵介绍招标项目招标情况，包括采购方式，发布媒体，提交投标文件的投标人家数、投标人名称；

⑶宣布开标纪律；

⑷投标人进行在线解密（解密时间为提交投标文件截止时间后30分钟内）；解密未成功的，启动备份投标文件，未提供备份投标文件的，视为放弃投标；

⑸投标人填写并通过邮件发送方式递交《政府采购活动现场确认声明书》（见招标文件附件），递交时间为解密指令发出后30分钟内；

⑹采购代理机构做好开标记录，投标人在解密完成后点击【查看开标记录】查看开标记录，并在线确认开标结果；

6.1.4 投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形，应通过电子邮件、传真等形式向采购代理机构提出询问或回避申请；

6.1.5 开标会议结束。

6.2 资格审查

6.2.1 资格审查内容：

采购人或采购代理机构按招标公告内投标人资格要求及本章第3.4条资格审查文件的组成内容进行审查；

6.2.2 ▲资格审查：全部满足下表要求的投标人为合格投标人，否则资格审查不予以通过；

|  |  |  |
| --- | --- | --- |
| **序号** | **资格审查内容** | **审查因素** |
| 1 | 营业执照 | 营业期限在有效期内； |
| 负责人身份 | 1. 负责人身份证正、反面电子文档；  2. 和营业执照上的法定代表人或负责人一致； |
| 授权委托书及委托代理人 | 1. 是否按授权委托书格式内容填写且盖章；  2. 委托代理人的身份证正、反面电子文档； |
| 2 | 财务状况报告依法缴纳税收和社会保障资金 | 是否按《具有良好的财务会计制度、依法缴纳税收和社会保障资金的承诺函》格式填写且盖章 |
| 3 | 履行合同所必需的设备和专业技术能力 | 是否按《具有履行合同所必需设备和专业技术能力的承诺函》格式填写且盖章 |
| 4 | 无重大违法记录 | 是否按无重大违法记录声明书格式填写且盖章 |
| 5 | 信用信息查询 | 1. 查询网址：  ⑴信用中国（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）  ⑵中国政府采购网（[www.ccgp.gov.cn](http://www.ccgp.gov.cn)）  2. 核对事项：  有无被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；  **注：**信用信息已修复的，以修复后的信息为准。 |
| 6 | 特定资格条件（若有） | 提供特定资格条件相关证书电子文档。 |
| 7 | 联合体（若有） | 1. 是否按联合体协议书格式内容填写且盖章；  2. 联合体各方资料是否齐全；  3. 联合体各方资料审查内容按上述要求提供，委托书由主办方提供一份。 |
| **注：以上资料内容须清晰可辨的，模糊不清造成资格审查不予以通过，由投标人自行负责；** | | |

6.2.3 经资格审查后合格的投标人不足三家的，不得进入评标，并按相关规定重新组织采购。

6.3 评标

6.3.1 评标办法：见投标人须知前附表（一）；

6.3.2 评标委员会由采购代理机构组建：评标委员会由评审专家或采购人代表和评审专家组成，成员人数为5人以上单数，其中评审专家不少于成员总数的三分之二，评审专家按规定从评审专家库中随机抽取。如有特殊情况的，按相关规定组建评标委员会；

6.3.3 评标由评标委员会负责，评标委员会应当遵循公正、合理、科学、择优的原则，严格按照招标文件确定的评标办法和评标细则进行评审和评分；

6.3.4 评标流程：符合性审查、资信商务及技术文件评审、报价文件评审；

6.3.5 符合性审查

⑴评标委员会对投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应，实质性响应是指投标文件符合招标文件规定的实质性内容、条件和规定；

⑵通过符合性审查不足三家的，除采购任务取消情形外，按相关规定重新组织招标。

6.3.6 资信商务及技术文件评审

⑴评标委员会依据招标文件的规定，对各投标人的资信商务及技术文件进行评审，其中客观部分应统一意见后统一给分，其他技术部分由评委委员会对各投标文件进行比较和必要的澄清，若有演示（讲解）环节要求的和资信商务及技术文件评审同步进行，演示（讲解）顺序由政采云系统自动生成循序进行，并根据澄清、演示、样品等情况按评审细则进行独立打分；

⑵各投标人的资信商务及技术得分，为各评审专家对该投标人的评审得分结果汇总后的算术平均数。

6.3.7 报价文件评审

⑴评标委员会依据招标文件的规定，对各投标人的报价的完整性、合理性进行审查，必要时可要求投标人对其报价做出澄清、说明；

⑵报价修正；

⑶政府采购政策价格扣除；

⑷评审委员会根据投标人的报价和评审标准，计算各投标人的报价得分。

6.4 投标文件的澄清、说明或补正

6.4.1 ⑴对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，**评标委员会通过政府采购云平台要求投标人作出必要的澄清、说明或者补正。电子投标文件的澄清、说明或者补正采用政府采购云平台交换数据电文，投标人提交的澄清、说明或补正的时间为30分钟（投标人务必在线等待，留意手机短信，及时在线澄清、说明或补正）。**投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容；

⑵投标人的的澄清、说明或补正将作为投标文件的一部分；

6.4.2 评审时评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，投标人在评标现场合理的时间内说明原因和提供证明材料；

6.4.3 不接受投标人主动对投标文件的澄清、说明或者补正。

6.5 报价错误修正

6.5.1 评标委员会对确定投标文件为实质上响应招标文件要求的，投标文件报价出现前后不一致的，按照下列规定修正：

⑴报价文件中开标一览表（报价表）内容与报价明细表相应内容不一致的，以开标一览表（报价表）为准（政采云系统开启报价若与报价文件不一致以报价文件为准）；

⑵报价文件的大写金额和小写金额不一致的，以大写金额为准；

⑶单价金额小数点或者百分比有明显错位的，以开标一览表（报价表）的总价为准，并修改单价；

⑷总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

⑸同时出现两种以上不一致的，按上述顺序修正；

⑹对不同文字文本投标文件的解释发生异议的，以中文文本为准；

⑺修正错误的投标报价，经投标人在线签章确认后产生约束力。调整后的投标报价对投标人具有约束作用。若投标人不接受修正后的投标报价，则其投标无效。

6.6 评标报告

6.6.1 评审结果汇总，投标人结果排序；

6.6.2 评标委员会根据全体评审成员签字的原始评审记录和评审结果编写评标报告，并推荐中标候选人或确定中标人；

6.6.3 评标报告由评标委员会成员签字确认生效，持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告；

6.6.4 评标结束后，采购代理机构通过中标公告的形式宣布评标结果。

七 ▲投标无效的情形

7.1 在开标时，如发现有以下情形之一的，其投标无效

⑴未按要求提交电子加密投标文件的；

⑵在规定时间内未解密电子加密投标文件或提交电子加密投标文件无法解密，且未按规定提交备份投标文件。

7.2 在符合性审查时，如发现下列情形之一的，其投标无效

⑴未按招标文件规定进行盖章的；

⑵未实质响应招标文件中带“▲”条款要求的投标文件；

⑶存在一个或一个以上备选（替代）投标方案的；

⑷投标人提交两份或两份以上内容不同的投标文件，未声明哪一份有效的。

### 7.3 在资信商务技术评审时，如发现下列情形之一的，其投标无效

⑴投标文件含有采购人不能接受的附加条款的；

⑵投标文件中提供赠品、回扣或者与采购无关的其他商品、服务的；

⑶评标委员会评定有非实质性条款负偏离超过招标文件规定项数的，项数要求见投标人须知前附表（一）；

⑷投标人已明知采购期间或之后企业将发生兼并改制，或提供的产品将停产、淘汰，或必须有偿使用专供的备品备件和试剂耗材的，及其他应当告知采购人可能影响采购项目实施或损害采购人利益的信息，不在投标文件中予以特别说明的；

⑸采购产品为政府强制采购的节能产品，投标人未提供节能产品认证证书的；

⑹投标文件内容不全或内容字迹模糊辨认不清的而导致评标无法正常进行（经评标委员会认定并允许其当场更正的笔误除外的）；

⑺违反国家及政府部门相关法律、法规、文件规定或经评标委员认定的其他属于重大偏离的。

### 7.4 在报价评审时，如发现下列情形之一的，其投标无效

⑴报价超过招标文件中规定的最高限价的；

⑵投标报价存在漏项或报价数量少于采购要求的，报价文件内容与对应资信商务及技术文件内容不一致的；

⑶评标委员会评定其投标的报价明显不合理或低于成本，有可能影响产品质量或者不能诚信履约的，在评标现场合理的时间内不能合理说明原因和提供证明材料的来证明其报价合理性的；

⑷拒不接受报价错误修正或报价错误修正后未签字确认的。

### 7.5 如有下列情形之一的，其投标无效

⑴投标人直接或者间接从采购人或者采购代理机构处获得其他投标人的相关情况并修改其投标文件；

⑵投标人按照采购人或者采购代理机构的授意撤换、修改投标文件；

⑶投标人之间协商投标文件的实质性内容；

⑷属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动；

⑸投标人之间事先约定由某一特定投标人中标、成交；

⑹投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交；

⑺投标人与采购人或者采购代理机构之间、投标人相互之间，为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为；

⑻不同投标人的投标文件由同一单位或者个人编制；

⑼不同投标人委托同一单位或者个人办理投标事宜；

⑽不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

⑾不同投标人的投标文件异常一致或者投标报价呈规律性差异；

⑿提供虚假材料谋取中标的。

### 7.6 如有下列情形之一的，可中止电子交易活动的情形

7.6.1 招标过程中出现以下情形，导致政府采购云平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购代理机构将中止电子交易活动：

⑴电子交易平台发生故障而无法登录访问的；

⑵电子交易平台应用或数据库出现错误，不能进行正常操作的；

⑶电子交易平台发现严重安全漏洞，有潜在泄密危险的；

⑷病毒发作导致不能进行正常操作的；

⑸其他无法保证电子交易的公平、公正和安全的情况

出现上述规定情形，不影响采购公平、公正性的，采购代理机构可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新组织采购。

八 中标和合同

8.1 中标

8.1.1 采购代理机构在评标结束后2个工作日内将评标报告提交采购人确认；

8.1.2 采购人应当自收到评标报告之日起5个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人；

8.1.3 采购人在收到评标报告5个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人；

8.1.4 中标人拒绝与采购人签订合同的，采购人可以按照评标报告推荐的中标人名单排序，确定下一候选人为中标人，也可以重新开展政府采购活动。

8.2 中标公告和中标通知书

8.2.1 采购代理机构应当自中标人确定之日起2个工作日内，在投标人须知前附表（一）规定的网址发布中标结果；

8.2.2 中标结果公告内容包括采购人和采购代理机构的名称、地址、联系方式，项目名称和项目编号，中标人名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求，中标公告期限以及评审专家名单，但不包括国家秘密或商业秘密；

8.2.3 中标公告期限为1个工作日；

8.2.4 采购代理机构将在中标结果公告中附中标通知书，视同向中标人发出中标通知书，同时中标人应在中标结果公告发布后签订合同前，赴政府采购代理机构项目负责人处领取书面中标通知书；

8.2.5 中标通知书发出后，采购人不得改变中标结果，中标人无正当理由不得放弃中标。否则将作为不良行为记录上报财政部门，由财政部门按相关法律法规给予处理。

8.3 履约保证金

8.3.1 履约保证金：见投标人须知前附表（一）。

8.3.2 中标人提供的服务和货物质量符合合同约定并经验收合格的，其履约保证金按规定要求由采购人无息退还。

8.4 合同

8.4.1 采购人应当自中标通知书发出之日起30日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

8.4.2 询问或者质疑事项可能影响中标（成交）结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

8.4.3 采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在浙江省政府采购网（zfcg.czt.zj.gov.cn）上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

九 其他事项

9.1 解释权

9.1.1 本招标文件解释权属采购代理机构；

9.1.2 采购代理机构对决标结果不负责解释。

第四章 合同格式

**第一部分 合同书**

项目名称：丽水市电子政务网络及数据安全服务项目

甲方： 丽水市大数据发展管理局

乙方：

签订地：

签订日期： 年 月 日

年 月 日， （采购人名称） 以 （政府采购方式） 对 （同前页项目名称） 项目进行了采购。经 （相关评定主体名称） 评定， （中标人名称） 为该项目中标人。现于中标通知书发出之日起三十日内，按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经 （采购人名称） （以下简称：甲方）和 （中标人名称） （以下简称：乙方）协商一致，约定以下合同条款，以兹共同遵守、全面履行。

**1.1 合同组成部分**

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 中标通知书；

1.1.3 投标文件（含澄清或者说明文件）；

1.1.4 招标文件（含澄清或者修改文件）；

1.1.5 其他相关采购文件。

**1.2 标的**

1.2.1 标的名称： ；

1.2.2 标的数量： ；

1.2.3 标的质量： 。

**1.3 价款**

本合同总价为：￥ 元（大写： 元人民币）。

分项价格：

|  |  |  |
| --- | --- | --- |
| 序号 | 分项名称 | 分项价格 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 总价 | |  |

**1.4 付款方式和发票开具方式**

1.4.1付款方式：

1.合同签订后，采购人在收到供应商开具发票之日起15日内支付第一个服务期经费的45%。

2.第一个服务期满后，根据绩效综合评价结果支付第一个服务期尾款。采购人在收到供应商开具发票之日起15日内支付该笔款项。

3.第二个服务期启动当月，采购人在收到供应商开具发票15日内支付第二个服务期经费的60%。

4.第二个服务期满后当月，根据绩效综合评价结果支付第二个服务期尾款。采购人在收到供应商开具发票15日内支付该笔款项。

5.第三个服务期启动当月，采购人在收到供应商开具发票15日内支付第三个服务期经费的60%。

6.第三个服务期满后当月，根据绩效综合评价结果支付第三个服务期尾款。采购人在收到供应商开具发票15日内支付该笔款项。

1.4.2 发票开具方式：

1. 乙方必须按照国家有关法律法规的规定如实足额向甲方开具并提供发票，乙方未提供发票的，甲方有权拒付款项。

**1.5 服务期限、地点和方式**

1.5.1 服务期限：三年（分三个服务期，每个服务期为一年），服务期起算之日为所有服务功能正式上线运行并通过甲方组织的会议评审之日。

1.5.2 服务地点： 丽水市 。

1.5.3 履行方式： 按本合同文件要求服务内容和服务要求 。

1.5.4 乙方无条件接受《丽水市大数据发展管理局信息化项目购买服务绩效评价管理细则(试行)》考评，同意甲方根据绩效考评结果支付款项，绩效考评扣款与违约金同时适用。

**1.6 违约责任**

1.6.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式履行，那么甲方可要求乙方支付违约金，违约金按每迟延履行一日的应提供而未提供服务价格的 0.05 %计算，最高限额为本合同总价的 1.5 %；迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；合同解除后，乙方应返还未提供服务部分的已收款项。

1.6.2 除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 0.05 %计算，最高限额为本合同总价的 1.5 %；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；合同解除后，甲乙双方按实结算服务费。

1.6.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段来影响对方当事人在合同签订、履行过程中的行为）或者欺诈行为（即：以谎报事实或隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同。

1.6.4 任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式。

1.6.5 除前述约定外，除不可抗力外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式。

1.6.6 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

**1.7 合同争议的解决**

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，可以选择下列第 1.7.1 种方式解决：

1.7.1 将争议提交丽水仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

1.7.2 向甲方住所地人民法院起诉。

**1.8 合同生效**

本合同自双方当事人盖章或者签字时生效。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 甲方（公章） | | | 乙方（公章） | | |
| 法定代表人 | (签字): |  | 法定代表人 | (签字): |  |
| 或被委托入 | 或被委托入 |
| 地 址： |  | | 地 址： |  | |
| 联 系 人： |  | | 联 系 人： |  | |
| 电 话： |  | | 电 话： |  | |
| 传 真： |  | | 传 真： |  | |
| 邮政编码： |  | | 邮政编码： |  | |
| 开户银行： |  | | 开户银行： |  | |
| 账 号： |  | | 账 号： |  | |
| 签约日期： 年 月 日 | | | 签约日期： 年 月 日 | | |

**第二部分 合同一般条款**

**2.1 定义**

本合同中的下列词语应按以下内容进行解释：

2.1.1 “合同”系指采购人和中标人签订的载明双方当事人所达成的协议，并包括所有的附件、附录和构成合同的其他文件。

2.1.2 “合同价”系指根据合同约定，中标人在完全履行合同义务后，采购人应支付给中标人的价格。

2.1.3 “服务”系指中标人根据合同约定应向采购人履行的除货物和工程以外的其他政府采购对象，包括采购人自身需要的服务和向社会公众提供的公共服务。

2.1.4 “甲方”系指与中标人签署合同的采购人；采购人委托采购代理机构代表其与乙方签订合同的，采购人的授权委托书作为合同附件。

2.1.5 “乙方”系指根据合同约定提供服务的中标人；两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购的，联合体各方均应为乙方或者与乙方相同地位的合同当事人，并就合同约定的事项对甲方承担连带责任。

2.1.6 “现场”系指合同约定提供服务的地点。

**2.2 技术规范**

服务所应遵守的技术规范应与采购文件规定的技术规范和技术规范附件（如果有的话）及其技术规范偏差表（如果被甲方接受的话）相一致；如果采购文件中没有技术规范的相应说明，那么应以国家有关部门最新颁布的相应标准和规范为准。

**2.3 知识产权**

2.3.1 乙方应保证其提供的服务不受任何第三方提出的侵犯其著作权、商标权、专利权等知识产权方面的起诉；如果任何第三方提出侵权指控，那么乙方须与该第三方交涉并承担由此发生的一切责任、费用和赔偿；

2.3.2 合同涉及技术成果的归属和收益的分成办法的，详见***合同专用条款***。

**2.4 履约检查和问题反馈**

2.4.1甲方有权在其认为必要时，对乙方是否能够按照合同约定提供服务进行履约检查，以确保乙方所提供的服务能够依约满足甲方之项目需求，但不得因履约检查妨碍乙方的正常工作，乙方应予积极配合；

2.4.2 合同履行期间，甲方有权将履行过程中出现的问题反馈给乙方，双方当事人应以书面形式约定需要完善和改进的内容。

**2.5 结算方式和付款条件**

详见***合同专用条款***。

**2.6 技术资料和保密义务**

2.6.1 乙方有权依据合同约定和项目需要，向甲方了解有关情况，调阅有关资料等，甲方应予积极配合；

2.6.2 乙方有义务妥善保管和保护由甲方提供的前款信息和资料等；

2.6.3 除非依照法律规定或者对方当事人的书面同意，任何一方均应保证不向任何第三方提供或披露有关合同的或者履行合同过程中知悉的对方当事人任何未公开的信息和资料，包括但不限于技术情报、技术资料、商业秘密和商业信息等，并采取一切合理和必要措施和方式防止任何第三方接触到对方当事人的上述保密信息和资料。

**2.7 质量保证**

2.7.1 乙方应建立和完善履行合同的内部质量保证体系，并提供相关内部规章制度给甲方，以便甲方进行监督检查；

2.7.2 乙方应保证履行合同的人员数量和素质、软件和硬件设备的配置、场地、环境和设施等满足全面履行合同的要求，并应接受甲方的监督检查。

**2.8 延迟履行**

在合同履行过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时提供服务的理由、预期延误时间通知甲方；甲方收到乙方通知后，认为其理由正当的，可以书面形式酌情同意乙方可以延长履行的具体时间。

**2.9 合同变更**

2.9.1 双方当事人协商一致，可以签订书面补充合同的形式变更合同，但不得违背采购文件确定的事项，且如果系追加与合同标的相同的服务的，那么所有补充合同的采购金额不得超过原合同价的10%；

2.9.2 合同继续履行将损害国家利益和社会公共利益的，双方当事人应当以书面形式变更合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

**2.10 合同转让和分包**

合同的权利义务依法不得转让，但经甲方书面同意，乙方可以依法采取分包方式履行合同，即：依法可以将合同项下的部分非主体、非关键性工作分包给他人完成，接受分包的人应当具备相应的资格条件，并不得再次分包，且乙方应就分包项目向甲方负责，并与分包供应商就分包项目向甲方承担连带责任。

**2.11 不可抗力**

2.11.1如果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；

2.11.2 因不可抗力致使不能实现合同目的的，当事人可以解除合同；

2.11.3 因不可抗力致使合同有变更必要的，双方当事人应在***合同专用条款***约定时间内以书面形式变更合同；

2.11.4受不可抗力影响的一方在不可抗力发生后，应在***合同专用条款***约定时间内以书面形式通知对方当事人，并在***合同专用条款***约定时间内，将有关部门出具的证明文件送达对方当事人。

**2.12 税费**

与合同有关的一切税费，均按照中华人民共和国法律的相关规定缴纳。

**2.13 乙方破产**

如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方终止合同且不给予乙方任何补偿和赔偿，但合同的终止不损害或不影响甲方已经采取或将要采取的任何要求乙方支付违约金、赔偿损失等的行动或补救措施的权利。

**2.14 合同中止、终止**

2.14.1 双方当事人不得擅自中止或者终止合同；

2.14.2合同继续履行将损害国家利益和社会公共利益的，双方当事人应当中止或者终止合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

**2.15 检验和验收**

2.15.1 乙方按照***合同专用条款***的约定，定期提交服务报告，甲方按照***合同专用条款***的约定进行定期验收；

2.15.2 合同期满或者履行完毕后，甲方有权组织（包括依法邀请国家认可的质量检测机构参加）对乙方履约的验收，即：按照合同约定的标准，组织对乙方履约情况的验收，并出具验收书；向社会公众提供的公共服务项目，验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告；

2.15.3 检验和验收标准、程序等具体内容以及前述验收书的效力详见***合同专用条款****。*

**2.16 通知和送达**

2.16.1 任何一方因履行合同而以合同第一部分尾部所列明的 联系方式 发出的所有通知、文件、材料，均视为已向对方当事人送达；任何一方变更上述送达方式或者地址的，应于 十 个工作日内书面通知对方当事人，在对方当事人收到有关变更通知之前，变更前的约定送达方式或者地址仍视为有效。

2.16.2以当面交付方式送达的，交付之时视为送达；以电子邮件方式送达的，发出电子邮件之时视为送达；以传真方式送达的，发出传真之时视为送达；以邮寄方式送达的，邮件挂号寄出或者交邮之日之次日视为送达。

**2.17 合同使用的文字和适用的法律**

2.17.1 合同使用汉语书就、变更和解释；

2.17.2 合同适用中华人民共和国法律。

**2.18 履约保证金**

2.18.1 采购文件要求乙方提交履约保证金的，乙方应按***合同专用条款***约定的方式，以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式，提交不超过合同价10%的履约保证金；

2.18.2 履约保证金在***合同专用条款***约定期间内不予退还或者应完全有效，前述约定期间届满之日起 / 个工作日内，甲方应将履约保证金退还乙方；

2.18.3 如果乙方不履行合同，履约保证金不予退还；如果乙方未能按合同约定全面履行义务，那么甲方有权从履约保证金中取得补偿或赔偿，同时不影响甲方要求乙方承担合同约定的超过履约保证金的违约责任的权利。

**2.19 合同份数**

合同份数按***合同专用条款***规定，每份均具有同等法律效力。

**第三部分 合同专用条款**

本部分是对前两部分的补充和修改，如果前两部分和本部分的约定不一致，应以本部分的约定为准。本部分的条款号应与前两部分的条款号保持对应；与前两部分无对应关系的内容可另行编制条款号。

|  |  |
| --- | --- |
| **条款号** | **约定内容** |
| 2.3.2 | 合同涉及技术成果的知识产权归甲方所有 |
| 2.5 | 结算方式和付款条件  结算方式：按合同书1.4.1执行。  付款条件：  针对每一年进行绩效考核，若绩效评价结果为优秀，根据合同支付尾款；评价结果为良好，则要求项目承接主体在1个月内对扣分项完善优化，之后根据合同支付尾款；评价结果为一般，则要求项目承接主体在1个月内对扣分项完善优化，优化后再由项目实施单位对其绩效复评，达到良好等级后按合同约定，扣减合同标的的5%；若绩效评价结果为较差，要求合同承接主体在1个月内根据绩效评价标准对扣分项完善优化，优化后再由项目实施单位对其绩效复评，达到良好等级后按合同约定，扣减合同标的的10%；如优化后绩效评价结果仍为较差，视为不合格项目，立即终止合同，并追究承接主体违约责任。 |
| 2.11.3 | 因不可抗力致使合同有变更必要的，双方当事人应在***三十个工作日内***内以书面形式变更合同 |
| 2.11.4 | 受不可抗力影响的一方在不可抗力发生后，应在***五个工作日内***以书面形式通知对方当事人，并在***十五个工作日内***，将有关部门出具的证明文件送达对方当事人 |
| 2.15.1 | 乙方在每个服务期截止前定期提交服务报告，甲方组织会议评审，根据绩效考核指标进行定期验收； |
| 2.15.3 | 检验和验收标准、程序等具体内容以及前述验收书的效力以乙方组织的会议评审为准 |
| 2.18 | 无履约保证金 |
| 2.19 | 合同份数6份，每份均具有同等法律效力。 |

第五章 投标文件格式

一 资格审查文件格式

### 1.1 资格审查文件封面格式

**投标文件**

|  |  |
| --- | --- |
| 投标文件名称： | 资格审查文件 |
| 项 目 编 号： |  |
| 项 目 名 称： |  |
| 标 项： | （若有） |
|  |  |
| 投标人全称（盖章）： |  |
| 投标人地址： |  |
|  | |
| 年 月 日 | |

### 1.2 资格审查文件目录

（格式自行设计）

### 1.3 有效营业执照复印件

内容要求：

提供有效的营业执照电子文档并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本电子文档并加盖单位公章；自然人的，则提供有效的身份证电子文档；

### 1.4 负责人身份证复印件

内容要求：

1、负责人身份证正、反面电子文档；

2、若有委托代理人的，则还应当提供授权委托书及委托代理人的身份证电子文档。

### 1.5 授权委托书格式

**授权委托书**

*（采购人名称）*：

我 *法定代表人（负责人）*系 *（投标人全称）* 的法定代表人（或负责人），现授权委托本单位在职职工 *（姓名）* 以我方的名义参加就贵方组织的 *（项目名称）（项目编号）（标项）* 的投标活动，并代表我方全权办理针对上述项目的投标、开标、评审、签约等具体事务和签署相关文件。

我方对委托代理人的签字或盖章事项负全部责任。

本授权书自签署之日起生效，在撤销授权的书面通知送达贵方以前，本授权委托书一直有效。委托代理人在授权书有效期内签署的所有文件不因授权的撤销而失效。

委托代理人无转委托权，特此声明。

投标人盖章：

日 期：

附：1、委托代理人工作单位： 职务：

身份证号码：　　　　　　　　　　 性别：

2、委托代理人身份证正、反面复印件：

|  |  |
| --- | --- |
| 正面： | 反面： |

**注：**1. 投标人为法人企业的，其负责人为其法定代表人；投标人为其他组织的，其负责人为法律、行政法规规定代表单位行使职权的主要负责人；投标人为自然人的，其负责人为自然人本人。

2. 若是负责人参会的，不需要提供此授权委托书。

### 1.6 具有良好的财务会计制度、依法缴纳税收和社会保障资金的承诺函格式

**具有良好的财务会计制度、依法缴纳税收和社会保障资金的承诺函**

*（采购人名称）*：

我方参与的 *（项目名称）（项目编号）（标项）* 的投标活动，我方郑重承诺，我方具有良好的财务会计制度、依法缴纳税收和社会保障资金，不偷逃税款和逃避缴纳社会保障资金。如有虚假，招标人可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标人盖章：

日 期：

### 1.7 具有履行合同所必需的设备和专业技术能力承诺函格式

**具有履行合同所必需设备和专业技术能力的承诺函**

*（采购人名称）*：

我方参与的 *（项目名称）（项目编号）（标项）*  的投标活动，我方郑重承诺，我方承诺具有履行合同所必需设备和专业技术能力。如有虚假，招标人可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标人盖章：

日 期：

### 1.8 无重大违法记录声明书格式

**无重大违法记录声明书**

*（采购人名称）*：

我方参与的 *（项目名称）（项目编号）（标项）* 的投标活动，我方郑重声明，我方参加本项目投标活动前三年内无重大违法记录（重大违法记录是指投标人因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚），符合《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》的规定。我方对此声明负全部法律责任。

特此声明。

投标人盖章：

日 期：

### 1.11 特定资格条件证明材料附件（若有）

（格式自行设计）

### 1.12 其他

（格式自行设计）

（投标人认为有利于其本次投标的其它资格证明材料等。）

二 资信商务及技术文件格式

### 2.1 资信及商务文件封面格式

**投标文件**

|  |  |
| --- | --- |
| 投标文件名称： | 资信商务及技术文件 |
| 项 目 编 号： |  |
| 项 目 名 称： |  |
| 标 项： | （若有） |
|  |  |
| 投标人全称（盖章）： |  |
| 投标人地址： |  |
|  | |
| 年 月 日 | |

### 2.2 资信商务及技术文件目录

（格式自行设计）

### 2.3 投标函格式

**投标函**

致：*（采购人名称）*：

根据贵方*（项目名称）（项目编号）（标项）* 的招标文件要求，正式授权下述签字人*（姓名和职务）*全权代表投标人*（投标人全称）*参加贵方组织的有关招标活动，并提交下述文件：

政府采购云系统提交电子加密投标文件 份；

通过电子邮件提交备份电子投标文件（打包压缩加密） 份；

据此函我方就本次投标有关事项郑重承诺如下：

1、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

2、我方承诺已经具备《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》中规定的参加政府采购活动的投标人应当具备的条件，并真实提供相关材料。

3、如果我方中标，将派出*（姓名及身份证号码）*，作为本项目与采购单位联系的项目实施负责人，联系手机号码： 。在项目实施过程中，并承诺项目实施负责人不更换，若确需要更换的，书面征得采购人同意后才准予更换。

4、我方的投标有效期自在开标日起 天内有效。如果在开标后规定的投标有效期内撤回投标，贵方可按相关规定处理我方。

5、我方在投标之前已经与贵方进行了充分的沟通，完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

我方愿意向贵方提供真实完整的任何与该项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

6、我方已详细审核全部招标文件，包括招标文件的澄清或修改文件（如有的话）、参考资料及有关附件，已经了解我方对于招标文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。

7、我方不是采购人的附属机构，并未为本项目提供整体设计、规范编制或者项目管理、监理、监测等服务。

8、我方将严格遵守《中华人民共和国政府采购法》第七十七条规定：投标人有下列情形之一的，处以采购金额5‰以上10‰以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动；有违法所得的，并处没收违法所得；情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

（一）提供虚假材料谋取中标、中标的；

（二）采取不正当手段诋毁、排挤其他投标人的；

（三）与采购人、其它投标人或者采购代理机构恶意串通的；

（四）向采购人、采购代理机构行贿或者提供其他不正当利益的；

（五）在招标采购过程中与采购人进行协商谈判的；

（六）拒绝有关部门监督检查或提供虚假情况的。

9、如中标，本投标文件至本项目合同履行完毕止均保持有效，我方将按招标文件及政府采购法律、法规的规定履行合同责任和义务。

10、以上事项如有虚假或隐瞒，我方愿意承担一切不利后果，并不再寻求任何旨在减轻或免除法律责任。

与本次投标有关的一切正式往来信函请寄：

地址： 邮编：

电话： 传真：

投标人盖章：

日 期：

注：按照本声明书要求填报。

### 

### 2.4 投标人资质

（格式自行设计）

投标人盖章：

日 期：

### 2.5 成功案例及业绩及相关证明材料格式

**成功案例及业绩（若有）**

投标人类似项目实施情况一览表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 采购人名称 | 产品或项目名称 | 采购数量 | 合同金额  （万元） | 签约及完成日期 | 附件页码 | | | 采购人联系人及联系电话 |
| 合同 | 验收报告 | 用户评价 |
|  |  |  |  |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |  |  |  |

此表后附合同复印件等相关证明材料。

投标人盖章：

日 期：

### 2.6 服务需求理解分析

（格式自行设计）

投标人盖章：

日 期：

### 2.7 服务能力

（格式自行设计）

投标人盖章：

日 期：

### 2.8 安全监管平台服务方案

（格式自行设计）

投标人盖章：

日 期：

### 2.9 网络安全一体化支撑平台服务

（格式自行设计）

投标人盖章：

日 期：

### 2.10 网络安全基础服务

（格式自行设计）

投标人盖章：

日 期：

### 2.11 网络安全加固服务

（格式自行设计）

投标人盖章：

日 期：

### 2.12 数据安全一体化支撑平台服务

（格式自行设计）

投标人盖章：

日 期：

### 2.13 数据安全基础防护服务

（格式自行设计）

投标人盖章：

日 期：

### 2.14 安全运行服务

（格式自行设计）

投标人盖章：

日 期：

### 2.15 安全体系保障服务

（格式自行设计）

投标人盖章：

日 期：

### 2.16 拟投入的项目班子格式

**拟投入的项目班子格式**

（格式仅供参考）

**项目负责人简历表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓 名 |  | | 年 龄 |  | | 学历 | |  |
| 职 称 |  | | 职 务 |  | | 拟在本项目任职 | |  |
| 毕业院校 | 年毕业于 学校 专业 | | | | | | | |
| 主要工作履历 | | | | | | | | |
| 时间 | | 参加过类似项目 | | | 担任职务 | | 业主及联系电话 | |
|  | |  | | |  | |  | |
|  | |  | | |  | |  | |

附：执业资格证书、职称证书、学历证书等电子文档证明材料

**项目班子一览表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名 | 职务 | 专业技术资格 | 证书编号 | 实施经验说明 |
|  |  |  |  |  |
|  |  |  |  |  |

附：相关人员的专业技术资格证书电子文档证明材料

投标人盖章：

日 期：

### 2.17 投标人需要说明的其他文件和说明

（格式自行设计）

投标人盖章：

日 期：

三 报价文件格式

### 3.1 报价文件文件封面格式

**投标文件**

|  |  |
| --- | --- |
| 投标文件名称： | 报价文件 |
| 项 目 编 号： |  |
| 项 目 名 称： |  |
| 标 项： | （若有） |
|  |  |
| 投标人全称（盖章）： |  |
| 投标人地址： |  |
|  | |
| 年 月 日 | |

### 3.2 报价文件文件目录

（格式自行设计）

### 3.3 开标一览表格式

**开标一览表**

项目编号：

项目名称： 标项：（若有）

|  |  |
| --- | --- |
| 名称 | 总报价（元） |
| 项目总报价 | 大写 （￥ ） |

**注：**

1. 具体价格明细详见《报价明细表》

2. 总报价应包括服务内容、包装、工时、运输、装卸、保险、税金、安装、调试与试运行、培训、保修、售后服务费、配套费、以及实施本项目所需的其他一切费用。

投标人盖章：

日 期：

### 3.4 报价明细表格式

**报价明细表**

（格式仅供参考，可以根据实际情况自行设计）

项目编号：

项目名称： 标项：（若有）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务内容 | 品牌  （若有） | 规格型号  （若有） | 单位 | 数量 | 单价（元） | 合价（元） |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 | …… |  |  |  |  |  |  |
| 总报价 | | 大写： （￥： ） | | | | | |

注：总报价应包括服务内容、包装、工时、运输、装卸、保险、税金、安装、调试与试运行、培训、保修、售后服务费、配套费、以及实施本项目所需的其他一切费用。

投标人盖章：

日 期：

### 3.5 中小企业声明函格式

**中小企业声明函（工程、服务）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加*（采购人名称）*的*（项目名称）*采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. *（标的名称）* ，属于*（采购文件中明确的所属行业）* ；承建（承接）企业为*（企业名称）*，从业人员 人，营业收入为 万元，资产总额为 万元①，属于（中型企业、小型企业、微型企业）；

2. *（标的名称）* ，属于*（采购文件中明确的所属行业）* ；承建（承接）企业为*（企业名称）*，从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

①从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

### 3.6 残疾人福利性单位声明函格式

**残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加 *（采购人名称）* 的项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：

### 3.7 监狱企业证明格式

**监狱企业证明**

**注：**须提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件

第六章 评标办法和细则

根据《中华人民共和国政府采购法》等有关法律法规的规定，并结合本项目的实际，特制定本办法，本办法只适用于本项目政府采购的评标。

一 总则

1.1 评标工作遵循公正、公平、科学、择优的原则确定中标候选人。评标委员会应严格按照招标文件的资信商务及技术和报价要求，对投标文件综合分析评价并编制评标报告。评审专家必须严格遵守保密规定，不得泄漏评标有关的情况，不得索贿受贿，不得参加影响评标的任何活动。

1.2 本次评标采用综合评分法，按最终得分由高到低顺序排列。最终得分相同的，按投标报价由低到高顺序排列；最终得分且投标报价相同的，按技术得分由高到低顺序排列。评标委员会按顺序推荐中标候选人。评分过程中采用四舍五入法，并保留小数2位。

二 评审一般规定

2.1 本次评标采用综合评分法，总分100分。

2.2 资信商务及技术分的权重为85%，评审分值为85分。评审专家对各投标人的资信商务及技术文件经充分审核，讨论后，其中客观部分（即资信商务部分）应统一意见后统一给分，其他部分（即技术部分）由评审专家独立评定打分。各有效投标人的资信商务及技术得分为各评审专家对该投标人的评审得分结果汇总后的算术平均值。

2.3 报价分的权重为15%，评审分值为15分，由评标委员会按各投标人报价统一计算。

2.4 投标人总得分=资信商务及技术得分+报价得分。

2.5 评审专家在规定的分值范围内打分，评分保留两位小数。

三 评审内容及标准

3.1 报价分（15分）

3.1.1 报价得分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其他投标人的价格分按照下列公式计算：

价格分=（评标基准价/投标报价）×报价权重×100

3.3.1 价格扣除：因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

调整后的投标报价＝投标报价×（1-扣除率）

3.2 资信商务及技术分85分，详细评分见下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **评分类型** | **评分项目内容** | **分值范围** | **备注** |
| 1 | **资信商务** | **投标人资质：**  投标人具有有效期内的ISO9001质量管理体系认证证书，提供证书扫描件，有得2分，没有不得分。  投标人具有有效期内的ISO20000服务管理体系认证证书，提供证书扫描件，有得2分，没有不得分。 | 0～4 |  |
| 2 | **成功案例及业绩：**  2019年1月1日（以合同签订时间为准）以来具有同类案例业绩的，每个案例需提供中标通知书及合同，每个案例得3分，最高得3分（同类案例是指与采购标的同品类的案例，由评审专家认定为准）。 | 0～3 |  |
| 3 | **技术部分** | **服务需求理解分析：**  根据投标人对本项目服务范围的了解情况和整体服务需求理解、分析的合理性和全面性，由评审专家评分，最高得8分。 | 0～8 |  |
| 4 | **服务能力：**  根据电子政务网络及数据安全服务项目性质，结合企业综合因素以及考虑企业长期稳定的持续服务支撑能力是否满足采购需求，由评审专家评分，最高得7分。 | 0～7 |  |
| 5 | **安全监管平台服务方案：**  根据投标人提供的服务方案，从资产管理服务、检查督查服务、安全评价服务、处置通报服务、知识库管理服务、应急保障服务、可视化展示服务、对接服务等几方面由评审专家判定能否满足采购需求，最高得5分。 | 0～5 |  |
| 6 | **网络安全一体化支撑平台服务：**  根据投标人对数据处理分析服务、网络资产普查服务、威胁态势感知服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 7 | **网络安全基础服务：**  根据投标人对流量采集服务、web应用监测服务、威胁情报数据服务、扫描评估服务、代码审计服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 8 | **网络安全加固服务：**  根据投标人对WiFi管控服务、非法外联检测服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 9 | **数据安全一体化支撑平台服务：**  根据投标人对数据安全资源运行、策略运行、风险运行、态势感知、一体化平台与数据安全基础能力联动服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 10 | **数据安全基础防护服务：**  根据投标人对多因子身份认证服务、数据水印溯源服务、数据日志审计服务、接口管控服务、数据分类分级服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 11 | **安全运行服务：**  根据投标人对驻场运行服务、检查评估服务、攻防演练服务、重保支撑服务、安全培训服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 12 | **安全体系保障服务：**  根据投标人对安全制度规范服务、安全评价管理指标体系服务、数据全生命周期安全行为研究服务的理解、实施方案的操作性是否满足采购需求，由评审专家评分，最高得5分。 | 0～5 |  |
| 13 | **拟投入的项目团队履历及能力要求：**  拟担任本项目的项目经理具备高级信息系统项目管理师、注册信息安全管理人员认证（CISO），两者同时具备的得4分，获得其中一项的得2分，两者都不具备不得分，最高得4分；  项目组成员具备注册信息安全专业资格证书（CISP），每人得1分，没有的不得分，最高得4分。  注：上述人员须提供资格证书扫描件及持证人员在本单位近三个月的社保缴纳证明材料附入资信商务及技术文件，否则不得分） | 0～8 |  |
| 14 | **1、讲解：**  投标人根据对项目采购需求的理解进行讲解，讲解内容应包含以下部分：  （1）安全监管平台服务内容讲解；  （2）网络安全一体化支撑服务内容讲解；  （3）数据安全一体化支撑服务内容讲解；  （4）安全运行服务内容讲解；  （5）安全体系保障服务内容讲解。  由评审专家根据讲解内容的完整性、成熟性是否满足招标需求进行判定评分，最高得5分。  **2、演示：**  演示内容详见采购需求中的安全监管平台服务、网络安全一体化支撑服务、数据安全一体化支撑服务。根据投标人演示的界面、功能、流程是否合理、完整、成熟，由评审专家根据演示情况是否满足招标需求进行判定评分，总体系统功能演示最高得10分；其中监管平台服务最高得3分，网络安全一体化支撑服务最高得3分，数据安全一体化支撑服务最高得4分。 注：仅有PPT没有DEMO的,演示部分最高得5分。 | 0～15 |  |

附件：政府采购活动现场确认声明书

**政府采购活动现场确认声明书**

*（采购代理机构名称）*：

本人经由 *（公司名称）* 法定代表人（负责人） ，合法授权参加*（项目名称）（项目编号）（标项）* 政府采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间 □不存在利害关系 □存在下列利害关系 ：

A.投资关系 B.行政隶属关系 C.业务指导关系

D.其他可能影响采购公正的利害关系（如有，请如实说明）

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位

□与其他所有供应商之间均不存在利害关系 □与（供应商名称） 之间存在下列利害关系 ：

A.法定代表人或负责人或实际控制人是同一人

B.法定代表人或负责人或实际控制人是夫妻关系

C.法定代表人或负责人或实际控制人是直系血亲关系

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

E.法定代表人或负责人或实际控制人存在近姻亲关系

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

I.其他利害关系情况

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、我发现 和 供应商之间存在或可能存在上述第二条第 项利害关系。

（投标人代表签名）：

年 月 日

注：1、投标人认为有利害关系和需要回避的人员，应提供相关证明材料，与本声明书一同提交。由采购代理机构和财政监督部门负责询问核查；

**2、[该声明书在投标文件解密后30分钟内以邮件方式发送至邮箱lssggzyjyzx@163.com](mailto:该声明书在投标文件解密后30分钟内以邮件方式发送至邮箱lssggzyjyzx@163.com)。**

**3、该声明书请各供应商在开标前提前准备好。**