

广东省政府采购

公开招标文件

采购计划编号：**440001-2026-17063**

采购项目编号：**ZZ0260087**

项目名称：广东省国土资源技术中心政务信息化运维（**2026**年）项目（基础设施及运行维护服务）

采购人：广东省国土资源技术中心（广东省基础地理信息中心）

采购代理机构：广东志正招标有限公司

第一章 投标邀请

广东志正招标有限公司受广东省国土资源技术中心（广东省基础地理信息中心）的委托，采用公开招标方式组织采购广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）。欢迎符合资格条件的国内供应商参加投标。

一.项目概述

1.名称与编号

项目名称：广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）

采购计划编号：440001-2026-17063

采购项目编号：ZZ0260087

采购方式：公开招标

预算金额：14,978,700.00元

2.项目内容及需求情况（采购项目技术规格、参数及要求）

采购包1(广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）):

采购包预算金额：14,978,700.00元

品目号	品目名称	采购标的	数量（单位）	技术规格、参数及要求	是否允许进口产品
1-1	计算机设备和软件租赁服务	专业基础设施服务	1.00(项)	详见第二章	否
1-2	计算机设备和软件租赁服务	成品软件租赁服务（许可）服务	1.00(项)	详见第二章	否
1-3	其他运行维护服务	基础设施运行维护、软件系统运行维护、其他运行维护服务	1.00(项)	详见第二章	否

本采购包涉及本国产品清单

序号	品目名称	采购标的	产品名称
不涉及			

本采购包不接受联合体投标

合同分包：允许合同分包

合同履行期限：第1种模式：以采购人确认的服务启动报审备案时间为服务起始时间，服务期为12个月。服务起始时间不晚于2026年10月1日。第2种模式：自2027年4月27日开始，至2027年10月27日止，共6个月。其中，一体化平台中云GIS模块的运行维护周期按第1种模式。具体见采购需求中的服务期限章节。

二.投标人的资格要求

1.投标人应具备《中华人民共和国政府采购法》第二十二条规定的条件，提供下列材料：

1）具有独立承担民事责任的能力：在中华人民共和国境内注册的法人或其他组织或自然人，投标（响应）时提交有效的营业执照（或事业法人登记证或身份证等相关证明） 副本复印件。分支机构投标的，须提供总公司和分公司营业执照副本复印件，总公司出具给分支机构的授权书。

2）有依法缴纳税收和社会保障资金的良好记录：提供投标截止日前6个月内任意1个月依法缴纳税收和社会保障资金的相关材料。如依法免税或不需要缴纳社会保障资金的，提供相应证明材料。

3) 具有良好的商业信誉和健全的财务会计制度：提供2024年或2025年年度财务状况报告或投标截止日前6个月内任意1个月的财务报表复印件；或银行出具的资信证明材料复印件。

4) 履行合同所必需的设备和专业技术能力：提供履行合同所必需的设备和专业技术能力情况，格式自拟。

5) 参加采购活动前3年内，在经营活动中没有重大违法记录：参照投标函相关承诺格式内容。重大违法记录，是指供应商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。（根据财库（2022）3号文，“较大数额罚款”认定为200万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于200万元的，从其规定）

2.落实政府采购政策需满足的资格要求：

采购包1（广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务））：本采购包预留合同总额的40%（或以上）专门面向中小企业采购。对于该预留份额部分，须由符合政策要求的中小企业承接。投标人可将满足预留部分金额的内容分包给一家或者多家中小企业，并在《分包意向协议》中载明分包承担主体、分包工作内容及金额，分包承担主体不得再次分包，投标时须提供《分包意向协议书》以及按规定填写《中小企业声明函》。若投标人为部分服务内容的供应商且为中小企业的，该部分内容无须分包。投标人与接受分包合同的中小企业之间不得存在直接控股、管理关系。（中小企业以投标人填写的《中小企业声明函》为判定标准，残疾人福利性单位以投标人填写的《残疾人福利性单位声明函》为判定标准，监狱企业须提供由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，否则不予认定。）。(2) 由中小企业承担的内容需至少包括：1.可视化屏租赁服务；2.安全和密码资源池租赁服务；3.全厅REDIS、CA设备及证书和安全产品特征库升级授权租赁服务；4.安全基础设施租赁服务；5.广东省自然资源一体化管理与服务平台（国土空间基础信息平台）云盘。

3.本项目特定的资格要求：

采购包1（广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务））：

1) 供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以资格审查人员于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网（<http://www.ccgp.gov.cn/>）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料）。

2) 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加本采购项目（或采购包）投标（响应）。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参与本项目投标（响应）。投标函相关承诺要求内容。

三.获取招标文件

时间：详见招标公告及其变更公告（如有）

地点：详见招标公告及其变更公告（如有）

获取方式：在线获取。供应商应从广东省政府采购网（<https://gdgpo.czt.gd.gov.cn/>）上广东政府采购智慧云平台（以下简称“云平台”）的政府采购供应商入口进行免费注册后，登录进入项目采购系统完成项目投标登记并在线获取招标文件（未按上述方式获取招标文件的供应商，其投标资格将被视为无效）。

售价：免费

四.提交投标文件截止时间、开标时间和地点：

提交投标文件截止时间和开标时间：详见招标公告及其变更公告（如有）

（自招标文件开始发出之日起至投标人提交投标文件截止之日止，不得少于20日）

地点：详见招标公告及其变更公告（如有）

五.公告期限、发布公告的媒介：

1、公告期限：自本公告发布之日起不得少于5个工作日。

2、发布公告的媒介：中国政府采购网(www.ccgp.gov.cn)、广东省政府采购网(<https://gdgpo.czt.gd.gov.cn/>)；广东志正招标有限公司 (<https://www.zztender.com/>)

六.本项目联系方式:

1.采购人信息

名称：广东省国土资源技术中心（广东省基础地理信息中心）

地址： 广州市海珠区磨碟沙路9号

联系方式： 钟先生020-87659062

2.采购代理机构信息

名称：广东志正招标有限公司

地址： 广东省广州市天河区龙怡路117号501、503、504、505、506房

联系方式： 020-87554618

3.项目联系方式

项目联系人： 李先生、吴小姐

电话： 020-87554618

4.技术支持联系方式

云平台联系方式： 020-88696588

开标评标服务专线： 020-88696599

采购代理机构：广东志正招标有限公司

第二章 采购需求

一、项目概况：

说明：

1、投标人须对所投项目为单位（有划分采购包的，则以采购包为单位）的标的物进行整体投标，任何只对其中一部分内容进行的投标都被视为无效投标。

2、本招标文件中，凡标有“★”的地方，投标人要特别加以注意，必须对此作出一一响应。若有一项带“★”的指标未响应或不满足，将导致其投标无效。

1.项目概况

1.1基本信息

1.1.1项目名称

广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务），以下简称“本项目”。

1.1.2采购人

广东省国土资源技术中心

1.1.3项目总体目标

夯实基础支撑，保障网络安全。确保广东省自然资源厅的重要信息系统、基础网络环境等的持续稳定运行，保障广东省自然资源厅重要信息化业务稳定运转；落实“数字政府”网络安全职责，确保保密、密评等监管合规，协同筑牢“数字政府”网络安全防线，提升省自然资源厅网络和数据常态化安全水平。

1.1.4服务地点

广东省广州市。

1.2项目背景

本项目在省自然资源厅政务信息化规划中定位于基础支撑和基础保障项目，提供基础硬件、基础软件等支撑保障能力，提供业务系统稳定运行所需的基础服务，保证系统的稳定性和可靠性，提高系统的效率和效益，为业务部门提供高效、安全、稳定的技术支持和业务支撑，以保障本单位工作的正常运转和高质量发展。基于智慧自然资源及前期项目建设成果，延续租赁硬件等基础设施，开展2026年基础设施及运行维护服务，为智慧自然资源建设及应用提供自主可控的基础支撑和运行保障。

2.项目预算

本项目总预算为人民币壹仟肆佰玖拾柒万捌仟柒佰元整（¥14,978,700.00），项目具体预算金额以省财政厅实际预算安排为准。

★供应商须对以下分项进行分项报价，无分项报价或分项报价超过分项预算的报价为无效报价，具体预算构成见下表。

项目名称	品目名称	分项	标的名称	预算 (万元)	是否面向中小企业预留分 包
专业基础设施服务	C23119900-其他租赁 服务	租赁费	可视化屏租赁服务	69.05	是
	C23119900-其他租赁 服务	租赁费	安全和密码资源池租赁服务	435.8	是
	C23110100软件租赁服 务	租赁费	全厅REDIS、CA设备及证书和 安全产品特征库升级授权租赁 服务	58.59	是
	C23119900-其他租赁 服务	租赁费	安全基础设施租赁服务	33	是
成品软件租赁服务 (许可) 服务	C23110100软件租赁服 务	租赁费	广东省自然资源一体化管理与 服务平台(国土空间基础信息 平台)云盘	35	是
基础设施运行维护 、软件系统运行维 护、其他运行维护 服务	C16070000运行维护服 务	维修(护)费	基础设施运行维护、软件系统 运行维护、其他运行维护服务	866.43	否
合计				1497.87	

3.服务期限

本项目服务期限适用模式详见下表。

序号	大类	小类	建设内容	建设内容	服务期限采用模式
1	基础设施服务	专业基础设施服务	可视化屏租赁服务	/	第（1）种模式
2			安全和密码资源池租赁服务	/	第（1）种模式
3			全厅REDIS租赁服务	/	第（1）种模式
4			CA设备及证书租赁服务	/	第（1）种模式
5			安全产品特征库升级授权租赁服务	/	第（1）种模式
6			安全基础设施租赁服务	/	第（1）种模式
7	软件开发服务	成品软件租赁服务（许可）服务	广东省自然资源一体化管理与服务平台（国土空间基础信息平台）云盘	/	第（1）种模式
8		基础设施运行维护服务	基础设施运行维护服务	/	第（1）种模式
9				广东省自然资源一体化数据库（自然资源三维时空数据库）运行维护服务	第（2）种模式

10	运行维护服务	软件系统运行维护服务	业务系统运行维护服务	广东省自然资源一体化管理与服务平台（国土空间基础信息平台）运行维护服务	第（2）种模式
11				广东省自然资源和不动产登记综合应用运行维护服务	第（2）种模式
12				广东省国土空间用途管制综合应用运行维护服务	第（2）种模式
13				广东省自然资源市场与资产监管综合应用运行维护服务	第（2）种模式
14				广东省测绘地理信息管理综合应用运行维护服务	第（2）种模式
15				广东省自然资源厅城市地质信息管理服务平台运行维护服务	第（1）种模式
16				广东省国土资源技术中心政务服务综合保障子系统运行维护服务	第（1）种模式
17			业务系统支撑环境运行维护服务	自然资源云专区数据库实例运维服务	第（1）种模式
18				自然资源云专区基础组件运行维护服务	第（1）种模式
19		其他运行维护服务	广东省自然资源业务网（业务网平面）网络平面运维服务	/	第（1）种模式

第1种模式：（1）以采购人确认的服务启动报审备案时间为服务起始时间，服务期为12个月。服务起始时间不晚于2026年10月1日。

第2种模式：自2027年4月27日开始，至2027年10月27日止，共6个月。其中，一体化平台中云GIS模块的运行维护周期按第1种模式。

4.服务内容

4.1基础设施服务

4.1.1专业基础设施服务

专业基础设施服务主要包括可视化屏租赁服务、安全和密码资源池租赁服务、全厅REDIS租赁服务、CA设备及证书租赁服务、安全产品特征库租赁服务、安全基础设施租赁服务等。

4.1.1.1可视化屏租赁服务

4.1.1.1.1服务背景

表3-1 可视化屏现有设备清单

序号	产品名称	规格型号	品牌	制造商	数量
1	LED显示屏屏体	HC1.2 II 600*337.5	艾比森	深圳市艾比森光电股份有限公司	10.935m²
2	拼接服务器	AXP 300N-A02U	艾比森	深圳市艾比森光电股份有限公司	1套
3	智能配电柜	QN	艾比森	深圳市艾比森光电股份有限公司	1套
4	LED显示屏安装结构	定制	艾比森	深圳市艾比森光电股份有限公司	1套
5	显示屏控制电脑	T4900	联想	联想集团	1台

6	会议平板（含PC模块、无线传屏器、红外智能笔、壁挂支架、移动支架）	BWB86-GI4C2	京东方	京东方集团	2套
7	网络云中控主机	DK-XPCIII	DIGIRATE	巨声视听科技（广州）有限公司	1台
8	中控扩展主机	DK-COM8P	DIGIRATE	巨声视听科技（广州）有限公司	3台
9	可视化移动操控终端	MatePad pro11	HUAWEI	华为技术有限公司	1台
10	交换机	华为 S5700-24TP-SI-AC	HUAWEI	华为技术有限公司	1台
11	10.1寸有线触摸屏	DK-15TP	DIGIRATE	巨声视听科技（广州）有限公司	3套
12	电源控制器	DK-P8	DIGIRATE	巨声视听科技（广州）有限公司	2台
13	36路数字视频矩阵	DH-36MIX	DIGIRATE	巨声视听科技（广州）有限公司	1台
14	4路HDMI输入卡	DH-4HDMI-I	DIGIRATE	巨声视听科技（广州）有限公司	6张
15	4SDI高清输入卡	DH-4SDI-I	DIGIRATE	巨声视听科技（广州）有限公司	1张
16	4路HDBaseT输入板卡	DH-4HDBT-I	DIGIRATE	巨声视听科技（广州）有限公司	1张
17	4路HDMI输出卡	DH-4HDMI-O	DIGIRATE	巨声视听科技（广州）有限公司	7张
18	4路HDBaseT输出卡	DH-4HDBT-O	DIGIRATE	巨声视听科技（广州）有限公司	1张
19	HDBaset延长器	DMDX-HDBT-T	DIGIRATE	巨声视听科技（广州）有限公司	4对
20	无线会议系统主机	XW1-Core	DIGIRATE	巨声视听科技（广州）有限公司	3台
21	无线会议主席单元	XW1-C	DIGIRATE	巨声视听科技（广州）有限公司	1台
22	无线会议代表单元	XW1-D	DIGIRATE	巨声视听科技（广州）有限公司	9台
23	无线会议话筒12只充电主机	BC12	DIGIRATE	巨声视听科技（广州）有限公司	1台
24	高清录播主机	ZQ-A6N	AVA	广州市奥威亚电子科技有限公司	1套
25	高清摄像机	AX-C22PN	AVA	广州市奥威亚电子科技有限公司	2台
26	录制面板	KP-8P3A	AVA	广州市奥威亚电子科技有限公司	1个
27	摄像机杆式升降吊架	定制	AVA	广州市奥威亚电子科技有限公司	2套
28	主扩音箱	PM12+	DIGIRATE	巨声视听科技（广州）有限公司	2只
29	主扩功放	MX700MK	DIGIRATE	巨声视听科技（广州）有限公司	1台
30	辅助音箱	PM10+	DIGIRATE	巨声视听科技（广州）有限公司	6只
31	辅助功放	MX350MK	DIGIRATE	巨声视听科技（广州）有限公司	3台
32	32路数字调音台	M32R	MIDAS	中山欧科电子有限公司	1台
33	音频处理器	DPA480	DIGIRATE	巨声视听科技（广州）有限公司	1台
34	自动反馈控制器	DFB280	DIGIRATE	巨声视听科技（广州）有限公司	1台
35	双手持无线话筒	AD100	DIGIRATE	巨声视听科技（广州）有限公司	3套

36	8路电源时序器	SP10	DIGIRATE	巨声视听科技（广州）有限公司	3台
37	专业机柜（42U）	42U，800*800，定制	图腾	广州励维	1台

4.1.1.1.2服务内容

因业务需要，在本项目中租赁可视化屏1年，租赁的设备可以选择延续租赁现有的设备，也可以选择租赁其他不同品牌的设备，但其参数要求不得低于现有设备参数要求，设备参数要求如下：

表3-2 可视化屏设备参数要求

产品分类	产品名称	技术规格要求	数量
------	------	--------	----

	LED显示屏	1.显示屏类型：LED类型采用SMD表贴3in1封装,LED 显示模组采用1010表贴封装，1R1 G1B 三合一全彩灯珠，灯珠尺寸为 1.0mm×1.0mm，自发光显示； 2.整屏尺寸：宽≥5.4米，高≥2.025米，面积≥10.935平方米，分辨率≥4320×1620，面积偏差允许3%以内。 ▲3基本参数：显示单元重量≤5.2kg，显示单元长宽比16:9，点间距≤1.25mm，像素点间距≤1.25mm；亮度均匀性≥99%；平均功耗≤1500W/m²。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。） 4.最高对比度≥10000:1；亮度≥600nit（自动/手动，0-100%无级可调，调节步长1级）；可视角度：水平≥170°，垂直≥170°；刷新频率≥3840Hz(420-4880 可调)，灰度等级：≥16bit。 5.色度均匀性：在±0.001 Cx,Cy之内；色准：ΔE≤0.9；色域：≥120% NTSC；像素中心间距差≤1%，LED像素失控率≤1/1500000。 6.电源带PFC高功率因数，功率因数≥0.95，转换效率≥88%；峰值功耗：≤500W/m²，平均功耗：≤166m²，宽电压AC100-240V，50/60Hz，具有带有智能（黑屏）节电功能，开启智能节电功能比没有开启节能50%以上，能源效率值≥3cd/W，睡眠模式功率密度值≤125W/m²。 7.箱体平整度：≤0.05mm，箱体间隙≤0.05mm，软件具有一键调节亮暗线功能：暗线修复、隐亮消除；模组支持X/Y/Z 三轴六向调节。 8.防眩光黑色电喷工艺，表面墨色一致性和散热性能好；焊盘采用沉金工艺处理，≥4层电路板结构设计，充分保证单模块安装的稳定性和抗氧化性；屏体正面为黑色亚光处理，屏幕表面不反射环境光，对比度更高，反光率≤1%；人眼视觉健康舒适度VICO 指数达到1级；蓝光危害辐亮度≤5.7 W/m²/sr，对人眼无伤害。 9.工作时间满足7×24小时连续工作无故障，平均故障恢复时间（MTTR）≤5分钟；4 档可调节恒流拐点电压（0.16V/0.24V/0.32V/0.4V），画面延时≤2ms。 10.具有控制系统对屏所有灯珠进行检测功能，检测后将坏点的数量及位置在软件上显示出来。接收卡、HUB板与模块之间采用并列连接，无排线设计，模组之间不级联，电源采用无电源线连接。 11.模组灯板采用双重接地功能，使用更加安全，当灯板出现短路时，灯板会熔断进入自动保护模式；屏体控制器与屏体间具有信号加密传输功能；具有六重备份技术：电源备份、接收卡备份、校正数据备份、接收卡文件备份、配置程序排布、环路备份；电源、接收卡采用1+1备份，整体提升产品的稳定性。 12.电磁兼容特性满足基于GB/T 9254-2008标准的CALSS B 级要求，电器绝缘显示屏符合CLASS1等级标准；PCB阻燃符合V-0要求，塑胶件阻燃符合V-0要求，内部线材阻燃符合V-0要求。 13. 提供光生物安全认证报告与蓝光危害安全认证证书。 14.屏体须通过CCC强制认证，非OEM产品。 ▲15. 可靠性：画面延时≤2毫秒（ms）；平均故障间隔时间（MTBF）≥5000小时（h）；平均故障恢复时间（MTTR）≤10分钟（min）。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	1套（≥10.935平方米）
--	--------	---	----------------

显示系统	拼接服务器	1.单台设备最大支持同时接入≥ 4个输入卡和≥ 2个输出卡。单路光纤最大支持传输≥ 8路网口数据，可同时支持网口传输和光口传输，板卡支持光口和网口之间的复制/热备。 2.前面板内嵌≥ 3.5英寸液晶显示屏，分辨率为$\geq 320 \times 480$，可通过显示屏显示设备运行参数与状态，包括：设备名称、设备接口连接状态、运行状态（温度、电压、风扇），以及IP地址。 3.单个输出板卡最大支持≥ 16个图层，每个图层可放大到4K显示；支持图层在输出接口间漫游，可进行图层参数设置，包括：无极缩放、图层画面截取、水平和垂直镜像翻转、冻结、叠加、图层优先级；可对图层无极缩放、图层全屏和自适应接口全屏。 4.单拼接屏幕支持≥ 1个OSD叠加显示，OSD可为文字或图片，最大尺寸支持$\geq 19200 \times 3240$，且透明度和位置可调，支持对字体间距、颜色、位置、透明度、运动特效等参数设置，支持任意比例缩放。可对输入图像画面添加台标（文字或图片），可调整台标文字与图片背景、位置。 5.屏幕画质调节支持≥ 4种调节模式标准模式、文档模式、会议模式、视频模式，每种模式下均支持护眼模式开关设置，护眼模式关闭时，可对亮度、对比度、饱和度、色调、色温、Gamma进行自定义调节。输出接口画质支持亮度、对比度、饱和度、色调、色温、Gamma调节，可添加≥ 22种测试画面图像，支持间距、速度、亮度调节。 6.支持设置≥ 2000个用户场景，场景可以设置为图片或视频，场景切换支持淡入淡出、直切效果，场景调取响应时间不大于60ms支持多场景分组和场景一键轮巡 7.支持用户权限分级管理和设置，超级管理员用户可分配用户使用权限。支持多用户同时在线编辑、控制、上屏操作，可预览其他用户操作。 8.内嵌BS拼接器配置软件，支持windows、麒麟(Kylin)、IOS、Android、Linux操作系统访问设备及交互操作。 9.为保证使用安全性，绝缘电阻试验应不小于270MΩ，泄漏电流试验应不大于0.1mA。	1套
	智能配电柜	1.功率$\geq 15kW$。 2.具备防雷、过压、过流、欠压、短路、断路以及漏电保护措施。 3.配电系统具有电源监视，温度，烟雾监控报警功能。 4.支持网络及串口控制，可通过PLC实现远程开关控制。	1套
	安装结构	1.用途：安装结构能满足LED高清显示屏的整体均匀平滑要求，用于精密固定箱体，保证拼接缝隙，嵌入式安装。 2.钢结构及装饰包边：依据现场美观性要求安装结构,钢架结构主材采用国标镀锌方管或环保型材。 3.焊接工艺：所有焊缝必须满焊，焊点打磨处理，喷刷≥ 3次防锈漆。 4.支持安装：前维护或后维护结构。	1套

控制电脑	1.处理器:处理器主频不低于2.93GHz。 2.主板: PCIe 3.0 ×16 显卡插槽。 3.内存: 4GB DDR4或以上内存。 4.硬盘: ≥1000G机械硬盘+≥120G固态硬盘。 5.显卡: 集成高清显卡。 6.网卡: 集成千兆以太网控制器。 7.键盘/鼠标: USB键盘、鼠标。 8.显示器: 19.5寸或以上宽屏液晶显示器。	1台
会议平板	1.有效显示面积≥1895.04mm(H)×1065.96mm(V), 大尺寸显示, 清晰画面。 2.一体机具有抗强光干扰功能: 抗光试验室外阳光照射试验将显示器置于室外阳光下, 用十点触摸笔在屏幕上划线十点划线连贯无断线无诡点。室内白炽灯照射试验将显示器置于200w高功率白炽灯照射下, 用十点触摸笔在屏幕上划线十点划线连贯无断线无诡点。 3.物理分辨率支持3840*2160, 亮度≥350nit, 对比度≥1200:1, 色彩度1.07B, 可视角度≥178°。 4. CPU: ≥1.5GHz ≥四核, GPU: RAM ≥3G, ROM ≥32G。 5.支持10bit 双路 LVDS(3840*2160)高清显示, 真彩色 OSD 人性化操作菜单。 6.屏占比不得低于87.8%, 四个边框宽度尺寸不得相差5mm以上。 7.一体机产品需要标配OPS接口, 方便后期随时插入OPS; 8.接口不得少于HDMI 2.0 IN≥3, HDMI2.0 OUT≥1,USB2.0≥2,DP≥1, USB-Touch≥3, USB3.0≥2, RJ45≥2, RS232≥1, PC-AUDIO 输入接口≥1, VGA≥1, Audio out≥1, TF Card≥1, OPS≥1, DVI≥1; 摄像头麦阵模块接口≥1。 9.为防止信号线脱落, 信号源接口必须具备DVI接口, 避免重要会议时信号中断。 10.摄像头需具备快速插拔功能, 摄像头与一体机连接采用PIN座插接方式, 不得采用飞线和外漏线等方式。 11.一体机面板为A+级别, 面板为原厂生产。 12.为保证操作便捷, 需具备全通道批注功能, 在批注时可以一键调出白板, 为防止误操作, 不接受使用手势拖拽等其他方式调出。 13.为保证一体机的信息安全, 一体机具有应用密码锁功能, 可对指定应用增加密码锁, 没有密码不得使用此应用。 14.一体机应满足《GB 4943.1-2022 音视频、信息技术和通信技术设备 第1部分: 安全要求》测试要求。 15.一体机必须符合强制性一体机认证制度, 需具备CCC认证。 16.一体机必须符合强制性一体机认证制度, 需具备产品节能认证证书。 17、会议平板含OPS。外形尺寸为200mmx119mmx30mm (各参数允许偏差值±5mm); OPS必须为intel标准定义的OPS。内存≥8GB; 硬盘≥256GB; 接口不得少于2个USB 3.0 端口, 2个 USB 2.0 端口, 1个HDMI端口, 1个RJ45接口, 1个RS232接口, 1Audio(MIC-IN&AUDIO-OUT); 电脑和电视组合化设计, 电脑主机采用插针式OPS结构, 无任何外接电源线和信号线。电脑主机可直接从电视机身的侧面抽拉式取出, 方便升级维护, 外部无任何可见连接线。 18、含无线传屏器、红外智能笔、壁挂支架、移动支架。	2台

中控系统	网络云中控主机	1、具备通过中国信息安全测评中心安全可靠测评的CPU，≥256M内存，≥1G Flash闪存。 2、不低于8路独立可编程的红外发射接口，支持控制多台相同或不同的红外设备。 3、不低于8路独立可编程RS-232/422/485控制接口，用户可编程设置多种控制协议和代码。 4、不低于8路弱电继电器接口。 5、不低于8路数字输入/输出IO接口。 6、具备网络通讯：AV-NET、AV-Link、Ethernet。 7、支持本地及远程多种控制方式。	1台
	网络云中控主机平台软件	支持IOS、安卓、WINDOWS控制端授权，人机交互控制界面，集网络控制，本地控制，云端备份控制更新等功能于一体。	1套
	中控扩展主机	1、支持RS-232接口，用于与主机通讯。 2、不低于8个COM1-COM8（RS-232）输出口用于信号的输出。 3、支持AV-NET四位网络接口。 4、支持DC12V电源适配器供电方式。	3台
	无线路由器	1、支持≥1路AV-NET网络控制接口，≥1路RS-232接口。 2、支持两种供电模式：DC 24V或AC 100-240V。 3、不低于8路独立节点控制接口，支持每路常开，常闭两种接口选择。 4、不低于8个防按错微动按钮控制。 5、支持RS-232、AV-NET以及以太网接口。 6、内置光电隔离模块。	1台
	电源控制器	1、支持≥1路AV-NET网络控制接口，≥1路RS-232接口。 2、支持两种供电模式：DC 24V或AC 100-240V。 3、不低于8路独立节点控制接口，支持每路常开，常闭两种接口选择。 4、不低于8个防按错微动按钮控制。 5、支持RS-232、AV-NET以及以太网接口。 6、内置光电隔离模块。	2台
	有线触摸屏	1、不小于15英寸64K真彩色TFT-LCD显示屏，分辨率不低于：800X600/1024X768。 2、支持有线双向收发控制功能。 3、内存不小于：1G SDRAM和32M Flash。 4、支持≥32位处理器，运行速度≥1GHZ。 5、支持USB接口、RS-232通讯端口、3.5立体音频端口。 6、支持画中画视频传输。 7、支持自定义界面。	3套
	可视化移动操控终端	1、7.9-8.3寸，≥32G，具备WIFI功能，支持2266*1488dpi分辨率。 2、支持信号切换、信号预览功能。 3、支持队列调控菜单功能、支持全中文界面操作，支持AW-NET设备专用协议中的SYSTEM-YUNV-18-5W内部数据通。 4、支持预案保存、调用。 5、支持全屏、2画面、4画面、3+1画面、6画面、9画面等布局，单屏布局整体实时预览功能。	1台

视频信号处理系统	36路视频矩阵	1、全数字化切换，每种无缝输出卡都能无黑屏实时无缝切换。 2、支持同时管理不少于5组拼接墙，画面支持任意开窗，漫游。 3、分辨率支持 $\geq 4K \times 2K$ ，支持DVI1.0协议，符合HDCP1.3标准，兼容HDMI1.4a。 4、全模块化，控制卡模块化，支持热插拔，能及时解决现场故障问题； 5、支持配套中控板卡，可以控制第三方设备。 6、前面板支持按键控制，和LCD状态显示，支持IP信息直接查看和修改。 7、插卡式结构设计，可灵活配置输入输出信号类型及信号通道数 8、支持冗余电源，设备运行更可靠。	1台
	4路HDMI输入卡	1、支持 ≥ 4 路HDMI-A母接口和3.5mm音频座。 2、支持快速无缝切换，无闪烁，无黑屏。 3、支持断电现场切换记忆保护功能，特有ESD静电保护功能。 4、支持音频为HDMI内嵌音频/外接模拟音频的选择输入。 5、支持图像参数修正。 6、兼容HDMI1.4b和HDCP1.4标准。 7、分辨率支持 $2560 \times 1440 @ 60Hz$ 超2K分辨率，带均衡20米线长。 8、支持热插拔，即插即用。 9、支持在线更新板卡程序，方便维护升级。 10、支持信号检测和温度检测，在线查询板卡信号状态和硬件状态。	6张
	4SDI高清输入卡	1、支持 ≥ 4 路SDI信号无缝输入。 2、支持 ≥ 4 路SDI环出。 3、支持输入分辨率自动识别：分辨率 $\geq 1920 \times 1080P @ 60Hz$ 的。 4、3G-SDI，HD-SDI和SD-SDI视频输入。 5、支持完全兼容HDTV；带宽高达19Mbps至2.97Gbps。 6、支持环出功能，方便本地监控。 7、支持热插拔，即插即用。	1张
	4路HDBaseT输入板卡	1、支持 ≥ 4 路高清RJ45接口无缝输入，高清音视频同步传输。 2、支持分辨率 $\geq 1080P @ 60Hz$ 高清输入分辨率。 3、支持HDCP协议、HDMI1.4b标准。 4、支持DVI/HDMI信号自适应。 5、支持远程POC供电。 6、支持热插拔，即插即用。	1张
	4路HDMI输出卡	1、支持 ≥ 4 路HDMI-A母接口和3.5mm音频座。 2、支持快速无缝切换，无闪烁，无黑屏。 3、支持断电现场切换记忆保护功能，有ESD静电保护功能。 4、支持模拟音频与HDMI内嵌音频同时输出；兼容HDMI1.3a的标准，HDCP1.3协议，DVI1.0协议。 5、支持倍线功能，分辨率支持 $\geq 1920 \times 1200 @ 60Hz$ 。 6、支持输出分辨率可调，支持图像参数修改。 7、支持热插拔，即插即用。	7张

	4路HDBaseT 输出卡	1、支持输出分辨率可设置，支持 $\geq 1920 \times 1200 @ 60\text{Hz}$ 搭配显示屏显示。 2、支持全部通道独立的亮度、对比度，饱和度、锐度、色调调节。 3、支持输出信号检测功能，并通过指示灯显示。 4、支持HDCP协议、HDMI1.3标准；可对标清视频进行去隔行处理网线传输支持 ≥ 150 米，无延时，无压缩传输。	1张
	HDBaset延长 器	1、支持可传输：50-100米。 2、支持音视频同步传输，EDID透传。 3、支持3D功能，RS232透传。 4、支持双向红外回控。 5、支持4K*2K向下分辨率全兼容。	4对
	无线会议系统 主机	1、一台主机可配 ≥ 12 台话筒，同时发言人数1-4个。 2、 ≥ 50 个WIFI通道可选。 3、 ≥ 200 个音频通道可选。 4、主机支持自动检测无干扰通道，设定音频接收通道，并能显示干扰信号强度，方便用户使用。 5、具备USB接口。支持U盘播放，会议录音。	3台
	无线会议系统 主席单元	1、具备视像跟踪功能。 2、防手机电磁波干扰。 3、内置电量监视功能，实时显示电池电量。 4、可选择1到4只话筒发言的先入先出模式。 5、红色多角度雾面指示灯设计,指示发言状态。 6、数字LCD显示屏，清晰明确地显示接收机的实时工作状态。 7、主席话筒具有主席优先键功能，可以关闭正在发言的代表单元。 8、抗干扰能力，能有效抑制由外部带来的噪音干扰及同频干扰。 9、高灵敏度金膜录音咪头，超指向性收音效果，有效拾音距离 $\geq 30-60\text{cm}$ 。	1台
	无线会议系统 代表单元	1、具备视像跟踪功能。 2、防手机电磁波干扰。 3、内置电量监视功能，实时显示电池电量。 4、可选择1到4只话筒发言的先入先出模式。 5、红色多角度雾面指示灯设计,指示发言状态。 6、数字LCD显示屏，清晰明确地显示接收机的实时工作状态。 7、主席话筒具有主席优先键功能，可以关闭正在发言的代表单元。 8、抗干扰能力，能有效抑制由外部带来的噪音干扰及同频干扰。 9、高灵敏度金膜录音咪头，超指向性收音效果，有效拾音距离 $\geq 60\text{cm}$ 。	9台
	无线会议话筒1 2只充电主机	1、每个槽位具备完全独立的充放电进程，消除记忆效应内建微处理器侦测负压差判停，辅以最大时间保护机制。 2、通用100V-240V电压。 3、完全的单回路设计可以对1到12只话筒任意充，放电充。	1台

高清录播主机	一、整体设计 1.主机架构：为保障系统运行稳定、安全，要求录播主机采用嵌入式架构设计，非PC、服务器架构。主机为标准1U机架式设备。 2.功能设计：要求主机具备录制、导播、自动跟踪、存储、点播、互动等多功能于一体，无需额外增加跟踪主机、互动主机。 3.节能环保：应具有嵌入式低功耗环保特性，需采用不高于DC36V安全电压供电，整机正常工作状态下功耗不超过40W。 4.低噪声设计：要求所投录播主机产生噪声最大值$\leq 28\text{dB(A)}$。 二、主机性能 1.视频输入输出：具备高清视频输入接口3G-SDI in≥ 4、HDMI in≥ 2；高清输出接口HDMI out≥ 3；且采集和输出分辨率均支持1080P@30fps。 2.视频编解码：支持标准H.264视频编解码协议，要求支持1080P30fps、720P30fps分辨率格式编解码。 3.POC：支持连接摄像机与主机之间通过一根SDI线进行供电、控制、视频信号同传，不接受使用转接器的方式。 4.音频输入输出：具备数字音频输入接口Digital mic≥ 6、线性音频输入接口Line in≥ 2；线性音频输出接口Line out≥ 2。 5.音频编解码：采用AAC音频编解码协议标准，并支持音频处理功能。 6.网络接入：具备标准RJ45网络接口，支持10/100/1000M网络自适应。并要求支持IPv4、IPv6双协议栈。 7.存储容量：内置不少于2T存储空间，用于录制视频文件的本地存储。 8.主机控制：具备Console控制接口≥ 2，支持RS232/422协议。 9.外设连接：具备USB 2.0接口≥ 2，可用于连接U盘等外设。	1套
	一.整体要求 1、软件架构：软件需采用B/S架构设计，使用浏览器通过网络即可访问软件后台进行管理应用。 2、自主知识产权：要求录播流媒体处理软件具备自主知识产权。 二.录播模块 1、录制存储：要求在断网情况下也可以对本地教室进行视频录制，并要求至少支持1080P高清分辨率录制，采用MP4视频格式封装。 2、分段录制：要求支持长视频分段录制的功能，可自定义视频文件分段时长，可在不结束录制的条件下自动按分段时长将课程视频文件分割录制成多个视频文件，提供不分段、30分钟分段、60分钟分段三种方式可选。 3、同步录制：要求支持U盘等外设设备接入主机后，实现本机与U盘同步录制保存的功能。 4、云台控制：支持摄像机云台控制技术，实现对接入摄像机的画面进行云台控制，包括画面上下左右移动、放大缩小变焦等操作。云台控制功能应具有鼠标快速定位功能，通过鼠标点击快速居中画面区域。 5、音频处理：要求内置音频处理模块，支持EQ均衡、AEC回声抑制、AGC自动增益、ANC噪声抑制等音频处理功能。 三.导播模块	

会议系统	录播流媒体处理软件	1、网络导播：要求支持通过浏览器访问录播主机进入导播界面，在导播界面实现对所有接入视频和录制效果画面的实时预览。不接受安装客户端软件进行导播的方式。 2、画面布局：提供双分屏、三分屏、画中画等录制布局，并支持自定义布局方式，支持多个视频图层自由叠加组合，自定义布局时可随意拖拉画面窗口 3、摄像机预置位：要求支持≥8个摄像机云台预置位设置。 4、字幕台标：要求录制模式下支持Logo台标、字幕设置，可自主上传Logo图标、编辑字幕内容。 四.直播模块 1、多流直播：要求支持RTMP和RTSP视频传输协议，并要求支持不少于3路RTMP同步推流直播。 2、直播模式：要求支持RTMP直播、TS直播、集控推流直播等不少于3种不同直播模式，以适应不同场景直播需求。 五.互动模块 1、互动协议：支持H.323、SIP标准视音频互动协议，便捷进行远程互动教学应用 2、互动要求：要求内置互动模块，无需额外部署MCU类设备即可支持“1+3”的互动授课模式，实现远程互动教学应用。同时也需支持会议互动模式，创建或加入大规模视音频实时互动。 3、双流互动：要求支持双流互动功能，支持教学场景信号与电脑课件信号以互相独立的信号进行传输，并最终接收端设备可通过两路HDMI接口将接收到的教学场景画面与电脑课件画面同时分别环出到两个显示设备上。 4、发言权限控制：通过录播主机的网络导播界面，需支持主讲端在互动过程中对其余互动参与者的发言权限进行控制，支持单人禁言/开启以及全场禁言/开启的控制方式。 六.管理模块 1、视频修复：支持硬盘格式化功能，支持对设备异常断电、宕机造成的损坏视频文件进行修复。 2、面板管控：支持接入控制面板，对录播设备进行唤醒、录制管理。	1套
------	-----------	--	----

	高清摄像机	1、视频输出接口：SDI≥1、HDMI≥1。 2、传感器类型：CMOS，1/2.5英寸。 3、传感器像素：有效像素≥207万。 4、焦距：≥22倍变焦。 5、水平转动速度范围：1.0° ~ 94.2°/s，垂直转动速度范围：1.0° ~ 74.8°/s，水平视场角：72.0° ~ 6.7°，垂直视场角：43.2° ~ 3.7°。 6、支持水平、垂直翻转。 7、背光补偿：支持。 8、数字降噪：2D&3D数字降噪。 9、预置位数量：≥255。 10、通讯接口：RS232/RS422≥1。 11、网络接口：RJ45≥1。 12、音频输入接口：Line in≥1。 13、USB接口：USB Type-A≥1。 14、支持的协议类型：VISCA。 15、编码技术：视频H.265、H.264。 16、电源支持：支持POC和DC12V电源适配器两种供电方式。	2台
	高清摄像机传输管理软件	1、摄像机管理软件采用B/S架构，支持通用浏览器直接访问进行管理。 2、支持曝光模式设置功能，包括自动、手动。 3、支持抗闪烁频率、动态范围、光圈、快门参数设置。 4、支持自动白平衡设置功能，红、蓝增益可调。 5、支持噪声抑制设置功能，支持2D、3D降噪。 6、支持摄像机图像质量调节功能，包括亮度、对比度、色调、饱和度。 7、支持摄像机控制功能，包括云台控制、预置位设置与调用、焦距调节等。	2套
	录制面板	1、在讲台上镶嵌式安装方式。 2、控制接口：RS232。 3、信号指示灯：支持。 4、支持一键式系统电源开关控制。 5、一键式录制、停止、锁定电脑信号。 6、支持本地录播全自动的开启、关闭控制。该功能同时支持录播模式和互动模式。 7、支持通过面板一键发起与远端设备互动连接。 8、支持对各画面的自由布局控制，包括单画面全屏、双分屏、三分屏、四分屏、画中画。	1个
	主扩音箱	1、≥12寸同轴扬声器。 2、频率响应：≥55Hz - 18kHz。 3、灵敏度：≥99dB。 4、最大声压级：≥131dB。 5、覆盖角度：大于或等于80°×60°(可旋转)。 6、功率：≥500W。	2只

扩声系统	主扩功放	1、根据扬声器匹配。2×950W/8ohm，2×1750W/4ohm，2×1800W/2ohm。 2、桥接8ohm 3500W,4ohm 3600W。 3、频率响应 (功率带宽 ±0.25dB): 20Hz-20kHz。 4、相位响应 (@1W 20Hz-20kHz): ±15度。 5、总谐波失真 (20Hz-20kHz): <0.05%。 6、互调失真 (SMPTE): <0.05%。 7、阻尼系数 (20-500Hz @8ohm):>500。 8、通道串扰 (20Hz-1kHz): >70dB。 9、电压增益: ≥35dB。 10、信噪比:≥105dB。 11、过热,短路,功率过载,电压过载保护。	1台
	辅助音箱	1、≥10寸多功能全频扬声器。 2、频率响应: 不劣于60Hz - 19kHz。 3、灵敏度: 不少于97dB。 4、最大声压级: 不少于127dB。 5、覆盖角度: 大于或等于80°×60°(可旋转)。 6、功率: 不少于350W。	6只
	辅助功放	1、根据扬声器匹配。2×650W/8ohm，2×1000W/4ohm，2×1000W/2ohm。 2、桥接8ohm 2000W,4ohm 2000W，70V 2×700W。 3、频率响应 (功率带宽 ±0.25dB): 20Hz-20kHz。 4、相位响应 (@1W 20Hz-20kHz): ±15度。 5、总谐波失真 (20Hz-20kHz): <0.05%。 6、互调失真 (SMPTE): <0.05%。 7、阻尼系数 (20-500Hz @8ohm):>500。 8、通道串扰 (20Hz-1kHz): >70dB。 9、电压增益: ≥35dB。 10、信噪比:≥104dB。 11、过热,短路,功率过载,电压过载保护。	3台
	32路数字调音台	1、不少于16路单声道输入，带经典模拟话放，不少于6路立体声。 2、不少于8个母线输出，不少于6个编组，LCR主输出。 3、40bit浮点信号处理，96kHz的采样率，192kHz的数模/模数转换。 4、不少于8个VCA/DCA编组，6个哑音编组。 5、不少于17个电动推子。 6、5寸以上显示屏。 7、USB 2.0可支持32×32通道的数字音频传输。 8、支持IOS、安卓等主流移动终端无线控制。	1台

	音频处理器	1、不少于4路输入8路输出。 2、32bit浮点运算，96KHz采样。 3、内置均衡器、分频器、压限器、延时器、滤波器、增益、相位。 4、可选 AES/EBU, SPDIF数字输入。 5、可通过USB以及EtherNet连接 PC。	1台
	自动反馈控制 器	1、采样率不低于32kHz。 2、频率响应范围不低于125Hz-15kHz。 3、失真不大于0.1 %。 4、增益不小于48dB。 5、共模抑制比不小于25dB。 6、信噪比不小于90 dB。 7、信号延迟不大于11ms。 8、最大电平不高于-42dBv。	1台
	双手持无线话 筒	1、自动选频接收。 2、红外自动同步。 3、可选频率不少于600个。 4、可预设不同频段数量不少于32个。 5、120MHz超宽带宽。 6、载波频段优于UHF 620-850MHz。 7、有效工作距离不小于100m。 8、信噪比不小于105dB。 9、谐波失真不大于0.7%。 10、频率响应优于45Hz-18kHz。 11、配套2支无线话筒。	3套
	电源时序器	1、受控通道数不少于8路。 2、最大输入电流不小于80A。 3、单路最大输出电流不小于16A。 4、每一路功率不小于3000W。 5、具有数字显示电压表。 6、可支持设备同时联机使用不少于8台。 7、支持多种控制方式：外部中控制器控制；串口控制RS232。	3台
	交换机	1、支持≥24个10/100/1000BASE-T电口,支持≥4个1000BASE-X SFP端口,支持AC。 2、支持IPv4/IPv6静态路由，RIP/RIPng。	1台
	机柜	42U专业网络机柜。	1台
专业音视频线 材及辅材	线材	要求：音频、视频、控制线等专业，符合质量标准。	1项

4.1.1.1.3服务成果

服务方案，应包括人员安排、质量保障计划、故障响应措施等内容；提交季度巡检报告、故障和问题处理记录（如发生）等。

4.1.1.2安全和密码资源池租赁服务

4.1.1.2.1服务背景

现有安全和密码资源池设备清单如下：

表3-3 安全和密码资源池设备清单表

序号	货物名称	规格型号	制造商名称	数量
1	高级持续性威胁检测系统	ND5000	北京安天网络安全技术有限公司	1台
2	流量分路器1	S-PATAP-24X	北京派网软件有限公司	1台
3	流量分路器2	S-PATAP-48X	北京派网软件有限公司	1台
4	业务网与政务外网强隔离交换	WI-DSES V2.0-10000-LP	广州智臣信息科技有限公司	2套
5	业务网终端网络准入控制	Leadsec-NAC-2200-E	北京网御星云信息技术有限公司	2台
6	云专区虚拟主机安全管理	EDR-EE-2000	杭州安恒信息技术股份有限公司	1套
7	业务网终端安全管控	Leadsec-EDR-6000-CONPR	北京网御星云信息技术有限公司	1套
8	Web应用安全保护1（万兆硬件）	Leadsec-10000WAF-S	北京网御星云信息技术有限公司	2台
9	Web应用安全保护2（千兆硬件）	Leadsec-6000WAF-FT	北京网御星云信息技术有限公司	1台
10	Web应用安全保护3（软件）	长亭雷池（SafeLine）WEB应用防火墙软件V2.0	北京长亭未来科技有限公司	1套
11	网页防篡改系统	Leadsec-SWAF	北京网御星云信息技术有限公司	1套
12	动态数据脱敏系统	LA-DM3000-M	北京网御星云信息技术有限公司	1套
13	静态数据脱敏系统	L-MaskServer-CLOUD	北京网御星云信息技术有限公司	1套
14	应用日志审计系统	DAS-LOG-600-C	杭州安恒信息技术股份有限公司	1套
15	数据库审计系统	LA-DAP-5000-SR、LA-DAP-5000-ER	北京网御星云信息技术有限公司	1套
16	万兆数据安全交换系统	WI-DSES V2.0-10000-P	广州智臣信息科技有限公司	2套
17	系统运维安全管控系统	LA-OS-FT-7600	北京网御星云信息技术有限公司	1套
18	数据库运维管控系统	L-VBH-CLOUD-Server、L-VBH-CLOUD-Portal、L-VBH-CLOUD-Dataserver	北京网御星云信息技术有限公司	1套
19	攻击欺骗诱捕系统	LD-CDS2000	北京网御星云信息技术有限公司	2台
20	网站云安全监测系统	LeadSec-WJ-JCB-Y	北京网御星云信息技术有限公司	1套
21	安全运营支撑平台	DAS-ABL-S2100	杭州安恒信息技术股份有限公司	1套
22	主机漏洞扫描系统	长亭洞鉴（X-Ray）安全评估系统软件V2.0	北京长亭未来科技有限公司	1套
23	云密码资源池管理平台	云密码资源池管理平台V2.0	三未信安科技股份有限公司	1套
24	密钥管理系统	密钥管理系统SYT1306	三未信安科技股份有限公司	1套
25	云服务器密码机	云服务器密码机SJJ1601	三未信安科技股份有限公司	2台
26	应用安全网关	应用安全网关NSAE	北京信安世纪科技股份有限公司	2台
27	签名验签服务系统	签名验签服务系统SRJ1909	三未信安科技股份有限公司	1套
28	文件加密系统	文件加密系统V6.0	广东七洲科技股份有限公司	1套
29	SSL服务器证书	GDCA SSL服务器证书	数安时代科技股份有限公司	2张
30	RSA服务器证书	GDCA RSA服务器证书	数安时代科技股份有限公司	2张

4.1.1.2.2服务内容

在本项目中租赁安全和密码资源池1年，服务期：已采购人确定的服务启动之日起计算，共12月，租赁的设备可以选择延续租赁现有的设备（系统），也可以选择租赁其他不同品牌的设备（系统），但其参数要求不得低于现有设备（系统）参数要求，现有设备参数要求如下：

4.1.1.2.2.1高级持续性威胁检测系统

表3-4 高级持续性威胁检测系统技术要求

序号	产品名称	技术要求	数量
		威胁捕获： 1.支持从包、流、会话、文件、元数据、网络行为、文件行为多个层次进行数据提取、监测和记录； 2.支持流式协议解析，支持对超大文件的留存，支持ACK包丢失容忍，乱序整理，MTU变化自适应； 3.支持基于真实通讯内容的协议识别，不受端口影响； 4.支持丰富的协议识别及解析，包括但不限于TFTP、NFS、HTTP、IMAP、SMTP、MSFFILE、RAWFILE、FEIQ、FTP、SMB、POP3、RAW、IEC_MMS、IEC_60870_104、RLOGIN、LDAP、ICMP、TELNET、UDP、TCP、ARP、BGP、SSH、TLS、DNS等协议； 5.支持隧道层剥离，包括但不限于IPinIP：4in4/4in6in4、ESP、VXLAN_GRE、L2TP、BGP、ETHERNET_LLC、STP、802.1Q（VLAN）、PPPOE：IPV4/IPv6、GRE、MPLS等； 6.可自定义协议和端口，满足特殊场景下的流量抓取； 7.支持流量过滤，包括但不限于IP白名单、协议白名单、邮件白名单、端口白名单； 8.支持基于真实文件格式的内容识别，不受扩展名影响，可识别伪装为其他格式的文件； 9.支持对逃避检测的加壳文件进行识别，壳识别不少于30种； 10.支持不少于370类文件格式的识别与还原，文件分类包括文档、可执行程序、脚本、压缩包、文本、图片、多媒体、软件数据； 11.支持用户手动配置需要进行还原、检测、深度分析、隔离的文件格式，支持设置还原文件大小上限； 12.支持提取MD5、域名、IP、端口、统一资源定位系统等信标，基于信标进行威胁检测、威胁统计，持续记录威胁事件，并支持通过信标快速定位威胁。	
		威胁检测： 1.支持注入攻击检测的能力，至少可检出XSS注入、SQL注入、宽字节注入、代码注入、文件注入、LDNP注入、XML实体注入等注入攻击； 2.支持检出 xss跨站脚本攻击、CSRF跨站请求伪造等跨站脚本攻击； 3.支持WEBshell检测的能力，至少可检出 Win.Backdoor.Chopper中国菜刀、冰蝎、一句话木马；支持JSP、PHP、ASP等格式的脚本检测； 4.支持其他类型的WEB攻击检测的能力，如目录遍历、弱口令、权限绕过、信息泄露、文件包含、文件写入攻击、DNS欺骗、钓鱼攻击、拒绝服务攻击、数据库登陆、非法路由、非法应用、可疑文件、非法web访问等攻击检测； 5.支持基于模型算法的HTTP隐蔽信道检测、IP分片隐蔽信道检测、DNS隐蔽信道检测等能力，可对单个隐蔽信道检测功能开启/关闭； 6.支持基于机器学习，语音学概率、传输数据熵值等元素的建模分析技术的DGA随机	

域名检测的能力；

7.支持UDP木马心跳报文异常分析模型检测，可开启/关闭；

8.具备APT事件的检测能力，可识别不少于120个APT组织，包含但不限于TA516、APT25、FruityArmor、Hamas、GCMAN、蓝白蚁、TA545、Luoxk、DustSquad、RasPite、MoneyTaker、FIN5等；

9.支持扫描行为的检测，包含但不限于TCP端口扫描、UDP端口扫描、ICMP分布式扫描，可通过界面进行阈值设置；

10.支持暴力破解行为的检测，包含但不限于SMB、FTP、HTTP、RDP、TELNET、SSH等暴力破解检测，可对单个爆破功能开启/关闭，支持通过界面进行阈值设置；

11.具备已知漏洞的漏洞利用行为检测，如操作系统漏洞、数据库漏洞、黑客工具、应用服务器漏洞。能够对检测到的非Oday漏洞给出漏洞编号；

12.支持Web服务器及插件的已知漏洞攻击检测，Web服务器至少应覆盖：apache、tomcat、lightpd、NGINX、IIS等；插件至少应覆盖：dedecms、phpmuadmin、PHPWind、discuz、echsop、vbulletin、wordpress、REST等；

13.至少内嵌一款反病毒检测引擎；

14.提供本地化静态检测能力，文件不上传云，完全进行本地化检测分析；

15.检测可支持不少于6万家族、1500万余变种的恶意代码；

16.支持对蠕虫、感染式病毒、木马、黑客工具、风险软件、灰色软件、垃圾文件、测试文件八大类威胁的检测，可识别威胁种类>860万种，规则数>5000万；

17.支持基于威胁类型、核心行为、依赖环境、恶意代码家族、变种号，对威胁予以精确命名，并提供家族信息；

18.支持基于IP、域名、统一资源定位系统等信标进行检测，发现远程控制、窃密回传、隐蔽信道等攻击行为；

19.具备行为分析能力，能够从文件、网络数据等提取重要信息，发现载荷行为；

20.支持对威胁事件的检测结果标签化，如木马程序、勒索软件、跨境通讯等；支持对网络军火的检测，并给出准确命名。

▲21.支持不少于30个的深度威胁（攻击）检测模块，支持对网络流量进行二次分析；支持DNS重绑定攻击检测能力，可获取记录DNS解析的IP地址与时间。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）

威胁分析：

1.支持对事件的相关属性，如事件的传输信息、网络行为、元数据、传输载荷、载荷行为、地理位置等信息等进行综合分析，生成详细的分析日志；

2.系统应提供基于被攻击资产、攻击源、恶意代码、失陷主机、恶意邮件、挖矿木马、勒索软件、拒绝服务、信息泄漏等不同维度的专项溯源分析能力；

3.支持被攻击资产分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组；

4.支持攻击源分析，以地图炮的形式展示攻击源分布情况，柱状图的形式展示攻击源TOP10。支持基于攻击源和攻击源事件列表两个维度进行分析。应具备攻击源传播分析的能力。以攻击源为视角进行分析，展示攻击源攻击行为产生过程中涉及的威胁类型、威胁行为以及攻击行为产生次数、攻击源所在地理位置；

1	高级持续性威胁检测系统	功能要求	5.支持恶意文代码分析，以柱状图、折线图的形式展示文件威胁类型TOP5分布情况、文件告警趋势等内容，支持基于恶意代码传播和恶意代码事件列表两个维度进行分析。应具备恶意文件传播分析的能力。以恶意代码名称的视角进行分析，展示恶意文件传播过程累计传播次数、威胁等级、威胁类型、威胁行为、自动判定结果、人工判定结果、恶意代码大小、最近发生时间等内容，并支持图形化呈现恶意代码传播范围。可查看恶意文件事件列表，以单次事件的形式展示文件名、文件MD5、文件类型、传输协议、威胁类型、威胁行为、自动判定结果、发生时间等内容。该维度应具备一键查看情报分析结果、一键旁路阻断及样本下载，同时可针对当前涉及的IP地址一键抓包审计及IP画像分析等能力； 6.支持恶意邮件分析，可对邮件相关属性，如邮件主题、发件人、收件人、抄送人、投递者、邮件正文、附件信息、附件行为信息等进行分析，发现钓鱼邮件等邮件通讯中存在的威胁； 7.支持挖矿木马专项分析，可从检测信标、挖矿行为、木马家族、矿池类型、资产IP、事件次数等方面对挖矿事件进行告警分析。应具备3种及以上虚拟货币的识别及告警能力，包括但不限于比特币、以太坊、门罗币等。具备15+以上挖矿木马家族的通信特征识别的能力，包括但不限于XMRig、CNRig、XMR-Stak、CoinMiner、BasedMiner、WatchBogMiner、云铲、ShadowBrokers、NSISMiner、Tor2Miner、Luminositylink、BitCoinMiner、Outlaw、NSABuffMiner、MyKings、SysrvHello、DarthMiner、8220挖矿团伙等。可查看挖矿木马事件告警详情，告警详情包括威胁等级、源/目的IP、协议类型、威胁类型、威胁行为及攻击状态，具备对检测信标、木马家族进行排名统计的能力，点击统计信息可关联展示相关告警列表信息。具备基础查询能力，包括但不限于以时间、资产IP、业务系统、检测信标、挖矿行为、木马家族、矿池类型等维度作为查询条件； 8.支持拒绝服务攻击分析，至少应具备Flood攻击检测的能力，包括但不限于DNS Flood、DNS REQUEST Flood、DNS RESPONSE Flood、SYN Flood、HTTP Flood、FIN Flood、RST Flood、ACK Flood、ACK Flood、ICMP smurf、ICMP Flood、UDP Flood；支持非法TCP标志位、非法TCP标志位、Ping Of Death攻击、Land攻击、WinNuke攻击、电子邮件炸弹等攻击检测。具备阈值配置的能力，单个功能可开启/关闭； 9.支持信息泄露分析，至少可检测QQ号码、密码、用户名等信息泄露事件，展示泄露信息类型、源IP、目的IP、协议类型、事件次数等信息，可查看威胁事件详情包括威胁等级、威胁类型、威胁行为、请求内容等信息，支持攻击阶段自动确认； 10.支持对DNS通讯相关属性，如解析域名、解析结果、请求内容、协议等进行分析，发现利用恶意域名、恶意IP实施的威胁事件； 11.支持对信息泄露的相关属性，如泄露信息类型、泄露账号、泄露源IP、泄露源端口、访问IP、访问IP所在地域、请求内容、协议等进行分析，发现信息泄露事件； 12.支持与沙箱产品联动，发现未知威胁；支持与情报产品联动，增强产品检测能力，提供更多分析信息； 13.支持对文档传输的相关信息，如文件来源、传输目的、文件统一资源定位系统、文件格式、文件大小、文件MD5、文件核心行为、威胁名称、传输协议、传输特征等进行分析，发现恶意文件传播事件；	1台
---	-------------	------	--	----

14.支持对建立C&C通道所使用的载荷、域名、远控服务器进行分析和发现，获取攻击者位置、使用的工具、资源等信息； 15.支持基于威胁画像的事件关联分析，生成关联分析报告，实现相关事件、攻击资源、攻击载荷、受害主机、漏洞利用情况的统一呈现； 16.支持对指定IP、协议或端口的原始流量进行捕获和留存，作为后续分析依据。支持同时添加多个IP进行重点审计； 17.支持对指定IP、协议或端口的原始流量进行捕获和留存，作为后续分析依据。支持同时添加多个IP进行重点审计；支持所有日志/威胁事件日志记录及导出，包括协议、源目的IP、端口、地理位置、上下行流量、信标（统一资源定位系统、IP、域名、文件）、标签、用户自定义标签；支持留存全部文件/威胁文件； 18.支持对高危IP或指定IP进行画像，生成IP画像报告，详细展示该IP的通联关系、域名及端口使用情况、攻击详情等信息。	
威胁告警： 1.支持对匹配的威胁事件进行告警，可根据网络环境、威胁能力来综合评定告警事件，显示捕获到的告警信息； 2.支持界面、邮件两种方式进行威胁告警：告警可展示告警名、告警时间、事件详情、关联事件、风险等级、处置状态等信息； 3.支持生成告警分析报告，对关联威胁事件的威胁信息进行汇总呈现，包括恶意代码传播关系、命令与控制关系、恶意文件、漏洞利用情况等。支持打印及导出； 4.支持手动更改告警处置状态，支持标识为待处理、处理中、已处理、忽略、已排除危险。支持手动合并告警。	
威胁呈现： 1.支持对指定时间段内设备捕获的事件数量、告警数量、捕获报文数量、监测流量趋势、各协议流量分布、文件格式分布情况进行统计与展示； 2.支持对威胁事件的事件描述、传输信息(源目的IP，源目的端口、协议类型)、网络行为、地理位置、威胁检测结果、资产信息、标签等信息等进行呈现，支持在线查看及导出； 3.支持通过丰富标签化结果，体现威胁类型、通讯特征、核心行为、自定义标识等信息。支持标签组合筛选，帮助管理分析人员快速定位威胁信息，提高分析效率； 4.支持手动批量导入资产信息，包括使用者信息、资产类型、部署信息、MAC等，支持事件与资产的精确对应； 5.支持按任意字段检索事件，支持模糊搜索，支持按与、或、非逻辑组合条件搜索； 6.支持展示匹配用户自定义检测场景的事件，如事件详情、匹配的自定义检测场景名称、自定义标识； 7.支持展示不同时间段内监测到的威胁整体情况，形成完整、全面的检测分析报告；支持导出为DOCX、PDF、HTML格式，支持报告打印；支持生成日报、周报、月报、年报； 8.支持威胁事件向网空威胁框架展示，包括但不限于attck，nsacss。	

威胁报表： 1.支持展示不同时间段内监测到的威胁整体情况，形成完整、全面的威胁检测分析报告； 2.支持展示当前网内威胁信誉、威胁涉及的资产、威胁类型、发现的恶意行为等威胁概览情况； 3.支持网内威胁整体趋势的展现，支持威胁分类统计、恶意文件统计； 4.支持对恶意代码传播路径分析和展现，至少可提供恶意代码二次传播路径的分析和展现； 5.支持网络军火的发现与呈现； 6.支持生成日报/周报/月报/年报； 7.支持报告导出为DOCX、PDF、HTML格式，支持报告打印。
日志管理： 1.支持威胁日志记录及导出，日志信息包括威胁事件的全要素记录，全流量时间、协议、源目的IP、端口、地理位置、上下行流量、风险等级、威胁等级、事件关联的全部威胁名称、检测详情、检测结果、信标（统一资源定位系统、IP、域名、文件）、告警状态、标签、用户自定义标签、协议详情。 2.支持记录运维操作日志功能； 3.支持威胁事件日志存储≥6个月； 4.支持日志导出为json格式； 5.支持配置日志存储策略，删除/启用最近特定天数的威胁日志。

		设备管理与升级： 1.支持用户角色（审核员、操作员、管理员）三员分离可对用户进行增删查改操作，支持生成运维操作日志； 2.支持安全登录认证、登录失败锁定、登录超时重新鉴别等安全策略与策略配置功能； 3.支持通过加密的SSL方式保证设备安全通讯； 4.支持导入授权，未授权/已授权/授权将到期以不同状态提示； 5.支持查看设备状态，监测设备配置情况。（1）展示CPU、内存、磁盘使用率，支持设置告警阈值；当工作状态异常时，产品能够发现、记录状态异常情况，并进行报警。（2）展示事件数量、捕获报文、监测流量大小、监控连接数； 6.支持检测引擎的配置，如不同引擎模块的开启与关闭、超时时间； 7.支持对还原文件格式、检测文件格式、样本隔离策略进行配置； 8.支持离线、在线（自动/手动）两种升级方式。不仅支持软件版本、病毒库的定期升级，也支持病毒库实时更新 9.支持时钟同步功能，支持配置时钟同步频率； 10.系统可提供与其他设备的数据联动接口，包括但不限于HTTP消息推送、SYSLOG日志发送、kafka消息推送、NAT日志联动、STIX2信息推动、IDMEF消息推送； 11.系统应具备针对资产所属业务系统的管理能力，可添加、修改、删除业务系统。业务系统至少应包含业务系统名称、业务系统责任人、责任人电话、责任人邮箱、业务系统关联资产数等内容； 12.系统应具备资产登记的能力，至少可记录来源于城市热点、锐捷身份认证和内网自动识别的资产、手动添加和批量导入资产的信息。资产信息至少可记录资产名、归属人、部署位置、业务系统、资产IP、资产MAC、资产类型、资产登记、资产来源、联系方式等信息； 13.支持配置、自定义规则、流量检测规则、用户管理、日志数据的备份与恢复； 14.具备至少两种系统登录方式，如账号密码验证登录、多因子身份认证登录。
	性能要求	支持接入流量镜像口、分光器。
		网络分析吞吐量≥10Gbps。
		ipv4、ipv6环境支持。
	其他要求	提供1年全模块特征库升级服务和1年维保服务。

4.1.1.2.2.2流量分路器

表3-5 流量分路器技术要求

序号	产品名称	技术要求	数量
----	------	------	----

1	流量分路器1	功能要求	流量复制转发： 1.支持基于端口输入\输出双向的流量复制； 2.支持基于流量分类规则的复制； 3.支持同时将报文输出到至少8个输出端口组以支持多个业务后端系统，且每个组可选择不同的分发策略； 4.输出组分流和接口镜像功能互不影响； 5.支持基于指定输出接口转发； 6.支持基于流分类结果转发； 7.支持大负载的环境下输出的报文流保序。	1台
			流量过滤： 1.支持源IP、目的IP、协议类型、源端口、目的端口、TCP Flag、输入接口号,VLAN ID等多元组匹配规则。匹配时可选择内层或者外层五元组信息，分流时可选择内层或外层五元组信息； 2.支持固定偏移字符串规则； 3.支持五元组规则命中使能截断动作。	
			负载均衡： 1.支持单一或级联设备同源同宿负载均衡； 2.支持负载均衡Linkdown接口动态分发； 3.支持负载均衡输出到指定的单个或多个输出端口组，端口组支持输出流量权重配比。	
			报文预处理： 1.支持纳秒级时间戳精度； 2.支持报文IP混淆脱敏，端口脱敏和载荷脱敏功能，且支持规则匹配后的脱敏动作； 3.支持报文截断，截断分端口可配置使能，截断长度从64到1500字节可配，截断后重封装CRC输出，截断处理性能≥160G； 4.支持1秒内的重复报文过滤，重复过滤功能可分端口开启， 5.支持全包内容对比去重方式，整体去重不低于40Gbps； 6.支持VLAN，MPLS，IP-IN-IP，GTP-U，GRE，VXLAN外层头的剥离和去封装；可修改输出报文的源/目的MAC地址或自定义协商字段，以便携带输入端口、命中规则号，或者精确时间戳等信息； 7.所有接口支持GRE隧道终结功能； 8.支持ERSPAN远程镜像接入；支持分片广播功能； 9.支持IP碎片报文的后续分片跟随头片动作转发。	
		性能要求	整机吞吐量：多IP、混杂应用流量（包含VLAN、MPLS、隧道、IP或者TCP选项等）下小包处理能力不低于240Gbps，流量复制性能不低于240Gbps。	
		规格要求	业务接口：≥24个10GE/GE光口；光纤模块：支持GE/10GE双纤LC光模块，电口RJ45光模块。	
		其他要求	提供1年维保服务和软件升级服务。	

2	流量分路器2	功能要求	流量复制转发： 1.支持基于端口输入\输出双向的流量复制； 2.支持基于流量分类规则的复制； 3.支持同时将报文输出到至少8个输出端口组以支持多个业务后端系统，且每个组可选择不同的分发策略； 4.输出组分流和接口镜像功能互不影响； 5.支持基于指定输出接口转发； 6.支持基于流分类结果转发； 7.支持大负载的环境下输出的报文流保序。	1台
			流量过滤： 1.支持源IP、目的IP、协议类型、源端口、目的端口、TCP Flag、输入接口号,VLAN ID等多元组匹配规则。匹配时可选择内层或者外层五元组信息，分流时可选择内层或外层五元组信息； 2.支持固定偏移字符串规则； 3.支持五元组规则命中使能截断动作。	
			负载均衡： 1.支持单一或级联设备同源同宿负载均衡； 2.支持负载均衡Linkdown接口动态分发； 3.支持负载均衡输出到指定的单个或多个输出端口组，端口组支持输出流量权重配比。	
			报文预处理： 1.支持纳秒级时间戳精度； 2.支持报文IP混淆脱敏，端口脱敏和载荷脱敏功能，且支持规则匹配后的脱敏动作； 3.支持报文截断，截断分端口可配置使能，截断长度从64到1500字节可配，截断后重封装CRC输出，截断处理性能≥320G； 4.支持1秒内的重复报文过滤，重复过滤功能可分端口开启，支持全包内容对比去重方式，整体去重不低于80Gbps； 5.支持VLAN，MPLS，IP-IN-IP，GTP-U，GRE，VXLAN外层头的剥离和去封装；可修改输出报文的源/目的MAC地址或自定义协商字段，以便携带输入端口、命中规则号，或者精确时间戳等信息； 6.所有接口支持GRE隧道终结功能； 7.支持ERSPAN远程镜像接入； 8.支持分片广播功能， 9.支持IP碎片报文的后续分片跟随头片动作转发。	
		性能要求	整机吞吐量：多IP、混杂应用流量（包含VLAN、MPLS、隧道、IP或者TCP选项等）下小包处理能力不低于480Gbps，流量复制性能不低于480Gbps。	
		规格要求	业务接口：≥48个10GE/GE光口；光纤模块：支持GE/10GE双纤LC光模块，电口RJ45光模块。	
		其他要求	提供1年维保服务和软件升级服务。	

4.1.1.2.2.3业务网与政务外网强隔离交换

表3-6 业务网与政务外网强隔离交换技术要求

序号	产品名称	技术要求		数量
1	业务网与政务外网强隔离交换	功能要求	支持基于单向光闸隔离的文件、数据库、接口等数据交换方式。	2套
			支持文件交换功能：支持通过ftp、http等方式进行文件单向、双向交换。支持文件交换完整性。	
			具备数据库交换功能。支持KingBase（人大金仓）、DM7（达梦）、高斯等数据库的同步交换。	
			支持接口化同步调用，可有效保障数据交换的实时性。支持以Web Service接口、REST API方式接收数据进行内外数据交换。支持基于XML报文的请求服务，实现内外系统的实时数据交换。	
			支持kafka数据交换，适配视频云、大数据平台等大规模消息交换业务。	
			支持文件常规检查功能，可对交换的文件进行基于正则表达式的文件名及后缀名（扩展名）检查。	
			支持基于文件特征的文件类型检查功能，即基于文件内容特征检查文件类型，当启用文件特征过滤功能时，文件特征符合策略的文件，将触发相应处理措施。	
			支持恶意代码扫描功能，可对文件进行病毒、木马等恶意代码检测。	
			支持文件内容关键字检查功能，可检查文件内容是否包含指定关键字。	
			支持XML报文附件检查功能，可对XML报文的附件解析后进行病毒、木马等恶意代码检测。	
		性能要求	文件交换：≥250MByte/s，数据库交换：≥10000条/s，接口调用：≥10000个/s。	
		规格要求	由内外安全交换系统和进出单向光闸等组成。	
			1.内外安全交换系统要求为2U标准机架式机箱，冗余电源； 2.网络接口：≥2个千兆电口，≥4个万兆SFP+插槽(含2个万兆多模SFP+模块)。	
			1.进出单向光闸要求为2U标准机架式机箱；冗余电源； 系统架构：采用2+1系统架构即内网单元+外网单元+专用单向隔离硬件。专用单向隔离部件通过利用光信号的单向传输特性以实现数据流的单向传输。 2.网络接口：内网≥6个10/100/1000M BASE-TX接口，≥2个万兆SFP+插槽(含2个万兆多模SFP+模块)；外网≥6个10/100/1000M BASE-TX接口，≥2个万兆SFP+插槽(含2个万兆多模SFP+模块)。	
		其他要求	提供1年维保服务和软件升级服务。	

4.1.1.2.2.4业务网终端准入控制

表3-7 业务网终端准入控制技术要求

序号	产品名称	技术要求		数量
1	业务网终端网络准入控制	功能要求	操作系统：支持双操作系统冷备，当常用系统出现故障，可以使用备用系统恢复。	2台
			部署要求：提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理。	
			准入控制： 1.支持VLAN隔离准入技术，实现无客户端下端口级准入控制 2.支持多种准入技术的复用，至少四种以上，如802.1x、DHCP、端口镜像、策略路由混合部署。	
			资源管理： 1.能够自动收集终端设备，包括：终端、手机、平板、交换机，并根据设备类型自动分类，能够自动绘制出网络拓扑图； 2.能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备； 3.支持可网管型交换机面板图形化展现各接口状态（单终端、无终端、多终端、关闭状态、Trunk口）； 4.支持远程加密协议管理；	
			移动终端管理：支持当前主流智能终端设备的安全准入控制，能够提供移动终端入网的设备注册、认证、授权功能	
			身份认证： 1.内置Radius认证服务实现本地用户名/密码认证，支持指定的Rdius服务器共享密钥，支持用户自注册功能，注册信息由管理员后台定义； 2.支持数字证书认证方式，支持证书的本地管理和发放，实现证书签发、管理和操作。	
			安全检查： 1.支持终端入网的安全基线检查、软件安全检查、账户密码安全检查、环境安全检查等检查项； 2.支持终端安装软件的检查和软件运行情况的检查，提供白名单、黑名单、红名单管理方式。 3.▲终端接入监控符合《信息安全技术 终端接入控制产品安全技术要求GA/T 1105-2013》（第三级）标准，（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
			泛终端安全防护： 1.支持实时监测泛终端指纹信息的变化，当泛终端指纹信息变化时，可及时对其进行告警或阻断； 2.支持检查终端是否发生网中网（NAT）行为、HUB行为，判断是否满足网中网的安全要求，并进行告警或阻断。	
		规格要求	标准2U机架设备，冗余电源；提供≥6个千兆电口、≥2个SFP插槽、≥2个万兆SFP+插槽；最大吞吐量≥6Gbps，终端准入控制授权数量≥1000个，存储容量≥2T。	
		其他要求	提供1年维保服务和软件升级服务。	

4.1.1.2.2.5云专区虚拟主机安全管理

表3-8 云专区虚拟主机安全管理技术要求

序号	产品名称	技术要求	数量
----	------	------	----

		统一管理平台：支持统一管理，适应云架构，提供统一管理平台,统一管理平台应支持在中标麒麟、统信、银河麒麟等操作系统上安装。	
		主机端（Agent）： 采用轻量级Agent，非检测处置状态占用CPU低于5%，内存低于80M；检测和处置状态占用CPU低于10%，内存低于160M。具备root权限守护进程，当Agent进程被kill后，能够在1分钟内自动拉起。	
		系统支持：支持通过中国信息安全测评中心安全可靠测评的64位图形界面操作系统，包括中标麒麟、银河麒麟、中科红旗操作系统。	
		资产管理： 1.支持点击资产所属类目下的相关资产进行资产信息查询；支持一键搜索，通过输入资产或主机关键词进行快速查询主机资产；支持主机视图、资产视图双维度查看。 ▲2.支持主机终端在线累积时长、离线累积时长、最近下线时间、总时长等信息展示能力。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
		容器： 支持采集容器信息，可采集容器的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等信息；	
		镜像： 1.支持自动对仓库镜像、本地镜像进行自动化扫描清点； 2.支持划分集群环境和非集群环境不同镜像类别，模拟业务环境提供多视角查看管理数据； 3.支持查看镜像详情，包括镜像名称、tag、镜像ID、镜像大小、author、创建时间、CMD、工作目录、入口点、环境变量等； 4.支持关联镜像来源和对应运行时资产； 5.支持展示镜像layer层信息，以及层关联构建命令，支持关联到对应的风险事件； 6.支持展示镜像风险评分，同时支持自定义风险评分规则； 7.支持标识可信镜像、基础镜像，并自动识别基础构建镜像和基础使用镜像类型； 8.提供镜像完整修复建议，用户可直接复制命令进行镜像风险修复。	
		第三方组件： 支持采集主机上的第三方组件信息，可采集第三方组件的版本、安装路径、相关网站等信息；支持的第三方组件有CKEditor、DedeCMS、Discuz、PHP、PHPMyAdmin、Struts2、WordPress、Zabbix等。	
		数据库： 1.支采集主机上的数据库信息，可采集数据库的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等； 2.支持主机及对应数据库双维度查看。	

1	云专区虚拟主机安全管理	功能要求	进程： 1.支持采集主机上的进程信息，可采集进程的路径、版本、hash值等；支持进程白名单设置、业务进程设置等； 2.可通过运行状态、进程标签、进程权限、是否系统进程、是否自启动、是否包管理安装、是否服务进程等多个维度进行进程信息的筛选。 账号： 支持采集主机上的账号信息，可采集账号的用户名、是否Root权限、Shell、状态、上次登录时间、可否交互登陆、登录方式、所属用户组、UID、密码过期时间、上次密码修改时间、终端、IP、用户主目录、上次密码修改时间、是否可交互登录等信息。 体检要求： 1.支持对主机进行即时安全体检及定时体检两种安全检测，检测的项目包括：系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门、反弹shell、异常账号、日志删除、异常进程、系统命令校验等； 2.安全体检检测出的问题系统可自动进行问题归类到漏洞风险及入侵威胁模块中。 批量体检：支持批量体检策略下发，通过设置体检的类型、体检的项目、体检的主机范围进行批量体检策略下发，并且支持定时体检策略与即时体检策略两种类型。 体检报告： 支持体检报告生成及导出，体检报告展示体检分数、健康指数，体检结果图表化展示及详细体检问题说明展示，可导出Word格式的体检报告。 监控要求： 可对主机开启各类监控包括登录监控、完整性监控、操作审计、进程监控、资源监控、性能监控。可从主机安全角度，全天候监控主机的运行情况，能确保第一时间发现服务器问题，帮助采购人快速发现安全风险和性能瓶颈。安全监测监测出的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中。 完整性监控： 监控文件和目录的完整性情况，包括文件被修改、删除和新增，支持设置文件夹和特定文件监控，支持白名单路径和文件类型。 会话监控： 监控主机上网络连接情况，采集会话连接的协议、本地地址、本地端口、外部地址、外部端口、进程等会话信息，并生成主机会话连接图表。 应急漏洞： 1.应急漏洞模块可采集近期爆发出的高危漏洞，通过应急漏洞的检测功能对主机资产进行快速检测，确认是否有资产受到影响； 2.支持漏洞和主机过滤，通过漏洞类型、风险等级、修复影响、影响软件、漏洞名称等进行漏洞过滤，通知主机分组、标签、状态、内核版本等进行主机过滤； 3.支持应急漏洞库设置，采集应急漏洞信息、统计应急漏洞总数； 4.支持检测任务设置，可创建检查任务，设置检测漏洞及检测主机范围。 配置缺陷： 具备操作系统、Web容器、数据库、及其他应用的配置缺陷检测能力。	1套
---	-------------	------	---	----

威胁分析： 展示不同类型威胁的攻击趋势和不同类型攻击威胁的详细攻击特征信息，并可以对攻击IP加入黑名单。
病毒查杀： ▲支持多引擎病毒查杀策略设置，包括但不限于默认引擎、深度扫描引擎、网马（网页挂马或网页木马）引擎的开关设置，并具备扫描缓存加速能力。（需提供报告封面具有 CM A 或者 CNAS 机构标识的第三方检测（检验或鉴定）报告复印件。）
网页后门： 展示安全体检和实时防护的webshell文件信息，包含webshell的类型、hash、路径，并且提供对webshell文件隔离、信任、下载和查看操作。
系统命令篡改： 支持安全体检检测到的系统命令被篡改的信息，包括篡改后的hash, 路径、篡改系统命令的危害和建议，并提供隔离和信任操作。
端口安全： 1.支持端口安全规则设置，可选宽松模式及严格模式，宽松模式下开放所有端口，只关闭规则中的端口； 2.严格模式下关闭所有端口，只开放规则中的端口； 3.支持TCP、UDP、ICMP、IGMP四种协议。
暴力破解防护： 1.提供全方位的暴力破解防护功能，支持FTP放暴力破解、远程桌面防暴力破解、MySQL数据库防暴力破解等暴力破解防护功能； 2.支持记录并拦截、记录不拦截两种模式。
僵尸蠕防护： 支持多引擎技术识别并查杀最新病毒，应至少包含四种查杀引擎；支持轻巧、中度、严格三种防护等级。
容器逃逸： 支持实时检测挂载逃逸、Cgroup逃逸、Procfs目录挂载逃逸、Ptrace逃逸、proc sys危险文件修改逃逸、重写Cgroup以访问设备逃逸、加载内核模块逃逸、利用binfmt_misc逃逸、内核提权逃逸等类型容器逃逸到宿主机的行为，提供详细的关联系统调用信息、进程信息和进程树信息。

		风险管理： 1.支持自定义配置节点镜像/仓库镜像扫描任务，支持本地镜像/仓库镜像精准匹配、模糊匹配选择指定项目内的镜像、或一批具备相似特征的镜像。支持设置镜像检查的风险类型，自定义仅扫描检查单个或部分类型风险，支持设置周期扫描时间和扫描范围； 2.支持镜像风险补丁检测，扫描镜像漏洞并关联到对应的修复补丁信息； 3.支持切换镜像视角和事件视角查看风险事件，直观查看每个镜像存在多少风险并推进修复； 4.支持对镜像内存在的恶意文件进行扫描，对镜像存在的木马病毒和webshell等恶意文件进行扫描，并给出修复建议； 5.支持对镜像中的敏感信息文件进行检查，如镜像中证书、key等敏感文件，检查结果至少包括：风险等级、文件信息、规则名称、检测依据等内容； 6.手动添加镜像扫描，可以手工添加指定的镜像进行安全扫描； 7.支持对容器内逃逸风险进行周期扫描，包括但不限于：由于敏感配置和敏感文件挂载导致的逃逸风险、由于特权容器导致的逃逸风险、由于不安全的Capability导致的逃逸风险、由于共享命名空间导致的逃逸风险； 8.支持对容器内弱口令风险进行周期扫描，支持对例如 ssh、elasticsearch、highgod b、influxdb、jenkins、kingbase_es、mongodb、mysql、postgresql、rabbitmq、redis、rsync、tongweb 等服务类型进行弱口令检查，并提供对应的检测依据来源和存在风险的用户名、密码信息； 9.支持用户自定义密码字典，支持配置字典内容、字典前缀、字典后缀和字典内容参数； 10.支持对所有容器资产进行应急漏洞进行周期扫描，例如：NacosRaft反序列化漏洞、Apachedubbo反序列化漏洞、用友NCuapjsjinvoke文件上传漏洞、致远OAsyncCon figManager远程代码执行漏洞、Fastjson<1.2.83远程代码执行漏洞等，提供详细的漏洞信息和影响面信息，并关联到对应的容器资产。
		进程白名单： 通过自学习或添加进程白名单，对非白名单进程的启动进行告警。
		报表生成导出： 可自定义时间区间分析生成全站攻击趋势、攻击类型分布、资产分布、漏洞风险分布、漏洞发现趋势、入侵威胁分布、入侵威胁发现趋势、新增监控异常分布、监控异常变化趋势等图表。
	规格要求	配置授权许可≥1000个点，含1年全模块特征库升级服务、维保服务及软件升级服务。

4.1.1.2.2.6业务网终端安全管控

表3-9 业务网终端安全管控技术要求

序号	产品名称	技术要求	数量
		产品形态： 软件形态，包含服务端和客户端组件，支持中标麒麟、银河麒麟、统信等通过中国信息安全测评中心安全可靠测评的64位图形界面操作系统，主要功能包括：数据传输加密、终端行为监控、环境安全检查、软件安全检查、关键配置安全检查、安全基线打分、可信白名单安全检查、响应处置等。	

1	业务网终端 安全管控	功能要求	基本要求： 1.支持C/S防护、B/S管理混合架构模式； 2.客户端支持在凝思、银河麒麟、中标麒麟、中科方德、深度等通过中国信息安全测评中心安全可靠测评的64位图形界面操作系统中安装部署； 3.支持服务器打包下载客户端； 4.支持服务器端远程升级、卸载客户端。	1套
			策略管理： 1.支持终端分组管理；支持分组信息导入、导出，至少包含：分组名称、操作系统版本、安装时间、主机名、IP地址、MAC地址、客户端安装时间等信息，便于资产管理和查看； 2.支持基于AI自学习能力提取终端信息一键自动生成标准策略并自动过滤高危内容。	
			日志报表： 1.支持终端采集信息、终端状态、终端风险告警事件的TOP统计与图形报表展示； 2.支持按照终端事件类型、分组、主机名称、IP地址、发生时间、上报时间进行筛选查询并可通过时间进行正序、反序展示；支持查询数据导出，至少支持HTML、EXCLE格式。	
			终端数据采集：支持终端当前、历史信息采集，至少包含：硬件、软件、进程、网络连接、服务、外设、文件、评分等主动基础信息采集能力。	
			安全基线检查： 1.支持环境安全检查，包括：终端补丁漏洞检查、防火墙状态检查、远程桌面状态检查、共享目录检查、共享打印机检查、共享IPC检查、屏保状态及时间检查、非法外联检查、终端密码弱口令检查； 2.支持根据安全基线规则内容对终端进行动态综合评分，实时掌握终端当前安全状态发现可疑终端。	
			安全白名单： 1.支持终端进程信息智能采集并与威胁情报碰撞检测进程安全性；支持通过进程名、路径、MD5设置进程白名单规则，保障终端进程在可信范围内运行； 2.支持终端网络信息智能采集并与威胁情报碰撞检测网络连接安全性；支持通过进程、协议、连入、连出、端口设置网络白名单规则，保障终端网络连接在可信范围内使用。	
			威胁检测： 1.支持对远程木马、漏洞利用、勒索软件、挖矿软件、主机扫描、恶意站点、暗网节点、网络判重等安全威胁进行检测并记录，日志至少包含：事件类型、终端信息、攻击者、危害等级、攻击组织、发生时间等对于已知威胁进行及时发现； 2.支持基于状态检测的链路层统一资源定位符过滤的方法。	

		威胁溯源： 1.支持通过威胁关联分析、AI场景分析、联动分析等方式还原多步骤攻击过程，建立攻击链，对安全事件进行深度分析和追踪，定位未知威胁攻击；支持留存安全事件元数据、关键样本信息，对威胁事件进行取证定位； 2.支持基于主机名称、IP、时间、方向、协议进程、端口等信息对终端安全威胁进行内网主机间流转横向溯源，明确安全威胁扩散方向和范围； 3.支持图形化直观呈现； 4.支持基于文件名称、时间、MD5、SHA1、SHA256等信息对终端文件传播行为进行溯源，明确恶意文件的攻击动向；支持图形化直观呈现。
		联动防御： 1.具备网络安全态势感知模块（系统或平台），将数据上报给网络安全态势感知平台进行EDR关联分析，并接收态势感知平台的反馈信息，进行对应的处置动作联动； 2.支持与威胁情报等外部平台导入的威胁指标进行关联分析，或与历史数据进行关联分析和威胁匹配，发现APT攻击等未知威胁或帮助威胁溯源。
	规格要求	配置不少于1000个终端授权，含1年全模块特征库升级服务、维保服务及软件升级服务。

4.1.1.2.2.7Web应用安全保护

表3-10 Web应用安全保护技术要求

序号	产品名称	技术要求		数量
1	Web应用安全保护1（万兆硬件）	功能要求	接入模式： 1.支持智能部署，上线WAF设备能够自动感知Web网站IP和端口； 2.支持NAT环境下的用户识别能力。 攻击防护： ▲1.具备Web恶意扫描防护的检测与防御功能，具体功能如下：可识别服务器的域名、操作系统、类型、编程语言、中间件、IP、端口等，并可根据感知信息优化防护策略；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。） 2.具备人机识别功能； 3.具备双引擎防护功能； 4.具有蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断； 5.具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截； 6.具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置； 7.具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响； 8.支持恶意地址主动屏蔽，提前免疫包括病毒网站或者攻击源地址的攻击。 安全联动： 1.支持和业务审计系统联动，满足用户对Web应用安全防护和审计需求； 2.支持和外联策略联动，满足用户对Web应用安全防护和外联策略联动需求； 3.支持和入侵检测系统联动，满足用户对网络流量镜像给IDS检测需求。	2台

		性能要求	网络吞吐率≥20Gbps，HTTP吞吐量≥10Gbps，最大并发HTTP连接数≥1000万。	
		规格要求	标准2U机架式设备，冗余电源；配置≥1个HA口、≥1个管理口、≥4个万兆SFP+插槽，≥1个接口扩展插槽（支持万兆接口扩展）。	
			提供1年全模块特征库升级服务、维保服务及软件升级服务。	
			产品应使用高性能硬件架构，在保证Web应用检测的高灵活性的基础上，实现高处理性能。	
2	Web应用安全保护2（千兆硬件）	功能要求	攻击防护： 1.具备Web恶意扫描防护的检测与防御能力； 2.具备人机识别功能； 3.具备双引擎防护功能； 4.具有蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断； 5.具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截； 6.具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置； 7.具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响； 8.支持恶意地址主动屏蔽，提前免疫包括病毒网站或者攻击源地址的攻击。	1台
			安全联动： 1.支持和业务审计系统联动，满足用户对Web应用安全防护和审计需求； 2.支持和APT进行动态联动，满足用户对Web应用安全防护和APT联动需求； 3.支持和外联策略联动，满足用户对Web应用安全防护和外联策略联动需求； 4.支持和入侵检测系统联动，满足用户对网络流量镜像给IDS检测需求。	
		性能要求	网络吞吐率≥10Gbps，并发HTTP连接数≥800万。	
		规格要求	标准2U机架式设备，冗余电源；配置≥1个HA口，≥1个管理口，≥8个千兆电口，≥8个千兆SFP插槽，≥1个接口扩展槽位，≥2个USB口，≥4T硬盘。	
			提供1年全模块特征库升级服务、维保服务及软件升级服务。	
			1.支持智能部署，上线WAF设备能够自动感知Web网站IP和端口； 2.支持NAT环境下的用户识别能力； 3.支持安装向导式部署，按照该部署方式可直接部署完成。	

3	Web应用安全保护3（软件）	功能要求 Web应用防火墙攻击检测能力： 1.支持非注入型SQL攻击检测，可基于“高危”、“高危和中危”或“所有级别”的攻击行为进行阻断或记录日志； 2.攻击检测模块中包含机器人检测，支持爬虫检测类型须包含字节跳动、yandex、无头谷歌浏览器； 3.支持信息泄露检测，检测内容须包括测试文件、备份文件、代码仓库和服务器敏感文件，可通过response检测信息泄露； 4.具备Oday漏洞防护能力，实现告警和拦截； 5.支持访问频率控制，访问频率限制规则支持观察模式和限制模式； 6.访问频率限制规则中，支持自定义频率，支持针对全站或具体的统一资源定位系统设置基于 IP 的访问控制策略，支持对该IP限定访问频率，或单位时间内对其进行封禁； 7.访问频率限制规则中，支持限制的目标类型包含IP、Session，支持手动输入要限制的IP列表或 Session 列表。 场景防护能力： 支持基于用户IP所在地理区域、IP清单、IP组、IP网段检测用户访问请求实现拦截转发至指定业务系统。 Web应用防火墙运维便捷性： 1.支持细粒度的告警阈值配置，包括出现大量web请求、出现大量web攻击、内存与磁盘使用率过高等。 2.支持攻击访问IP溯源，能够从Socket、X-Forwarded-For和任意Http头中获取访问源IP，其中X-Forwarded-For支持倒数第n层代理进行获取，n为可灵活自定义的数字。 3.攻击事件分析时，攻击检测日志应包含完整的事件信息，包括攻击类型、风险等级、命中策略，支持告警日志下载、告警加白、请求重放操作。 解码能力要求 1.为应对高级混淆攻击，需具备完善的编译解码能力，对解码后的内容进行语义分析，解码方式包括支持统一资源定位系统解码、JSON解码和Base64解码；16进制转换、二进制解码、PHP反序列化解析； 2.支持根据具体站点灵活设置开启或关闭解码方式。	1套
		性能要求 1.HTTP 吞吐量≥3.5 Gbps； 2.HTTP QPS ≥18,000； 3.HTTP CPS ≥16,000； 4.并发链接数 ≥ 1,000,000。	
		规格要求 产品形态及部署模式要求： 1.支持单机和集群部署，可实现动态扩容； 2.部署模式支持流量镜像、反向代理单机、反向代理集群； 3.提供1年全模块特征库升级服务、维保服务及软件升级。	

4.1.1.2.2.8网页防篡改系统

表3-11 网页防篡改系统技术要求

序号	产品名称	技术要求	数量
----	------	------	----

1	网页防篡改系统	功能要求	防篡改功能： 1.支持各类网页文件的保护，包括静态和动态网页以及各类文件信息； 2.支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码； 3.支持篡改后的自动恢复功能，恢复不依赖访问事件，直接由篡改动作触发恢复机制进行恢复； 4.配置完成后，系统后台运行，支持断线检测； 5.支持在断线情况下对网页文件目录的防护功能； 6.支持黑白名单设置功能，提供进程黑白名单设置； 7.支持对服务进行监控功能。	1套
			同步功能： 1.可以从本地或异地备份文件夹自动同步到监测目录内； 2.支持手工指定文件或文件夹从监测目录到指定目录的备份，支持增量备份功能； 3.支持通过管理端受限用户进行文件上传下载功能； 4.支持网络异常的自动恢复； 5.支持发布失败的自动重新发布； ▲6.具备基于SSL安全协议进行通信和文件传输的安全接入能力，保证通信过程安全性； （需提供第三方资质机构颁发的技术证明文件） 7.支持多虚拟主机/目录的并发同步功能； 8.支持跨操作系统平台的同步； 9.支持对web服务器的远程维护管理功能，如远程接管、远程唤醒、远程关机、远程用户注销等； 10.支持对服务器性能实时监控功能，包括：内存、CPU占用率等； 11.支持对服务器实时信息监控，包括：实时进程，服务信息，系统日志。	
			自身安全性： 1.系统各个模块之间、进程之间的通讯、交互和自身配置均采用加密传输和保护； 2.卸载时需要提供管理员口令才可执行； 3.支持对系统关键配置信息进行加密保护； 4.支持对备份目录文件的保护。	
			保护动态页面模块： 支持扩展保护动态页面模块，能够有效防止SQL注入攻击、跨站攻击、溢出代码攻击、对危险文件类型的访问、对危险系统路径的访问、特殊字符构成的统一资源定位系统利用、防止构造危险的Cookie等。	
		性能指标	报警方式：支持声音、邮件、报警提示框提示报警，对非授权用户篡改网页提供实时报警。 1.当网站文件遭到篡改恢复最短时间小于2ms； 2.能够保护站点的最大文件和目录的数量不限； 3.能够保护站点的最长路径不得小于10级； 4.运行过程中，被保护主机的CPU资源占用率和内存占用率小于2%。	
			产品为软件形态，支持中标麒麟、银河麒麟、统信等操作系统部署。	

		规格要求	C/S架构，可以支持多个客户端管理。
			采用基于文件过滤驱动保护技术、事件触发机制相结合方式。
			提供1年维保服务及软件升级。

4.1.1.2.2.9动态数据脱敏系统

表3-12 动态数据脱敏系统技术要求

序号	产品名称	技术要求		数量
1	动态数据脱敏系统	功能要求	数据兼容性： 1.支持达梦、人大金仓、高斯DB、神舟通用、TDSQL、TBASE等通过中国信息安全测评中心安全可靠测评的数据库； 2.支持Greenplum、Teredata数据仓库脱敏能力扩展； 3.支持对API数据网关/数据接口的实时脱敏功能，适用于基于RESTful风格的数据格式脱敏。	1套
			支持复杂场景和SQL脱敏： 1.支持IPV6的数据资产的动态脱敏； 2.支持复杂SQL请求的脱敏，包含但不限于：查询 *，嵌套和多层嵌套，连接（左连接、右连接、内连接）查询，比较查询、模糊查询、范围查询、分组查询等。	
			敏感数据智能发现： 1.系统内置不少于20类预定义敏感数据智能发现规则； 2.支持自定义扩展敏感数据特征，新扩展的敏感数据特征可以通过数据发现功能进行识别； 3.支持敏感信息的自动发现能力，能对姓名、地址、电话、手机号、身份证、统一信用代码、银行卡号等敏感信息智能识别； 4.敏感数据的特征库可以通过离线更新包的方式进行更新。	
			敏感数据访问审计： 支持对敏感数据访问的记录进行统计，用于回溯和查看敏感数据的访问频度和行为轨迹。	
			数据分类分级： 1.支持自定义添加数据类别，对数据进行分类脱敏，满足数据分类的业务及合规需求； 2.支持自定义添加数据敏感等级，对数据进行分级脱敏，满足数据分级的业务及合规需求。	
			脱敏算法： 1.内置脱敏算法，支持对常见敏感数据如姓名、地址、电话、手机号、身份证、统一信用代码、银行卡号等敏感数据进行脱敏； 2.支持置空、遮蔽等脱敏效果，系统内置脱敏算法总数不少于50种； 3.支持扩展随机、仿真脱敏算法； 4.支持在线添加自定义脱敏算法，满足用户对脱敏效果的个性化需求； 5.支持内置算法的离线更新。	
			行业模版： 内置常用行业脱敏模版，适用于特定行业的脱敏规则关联，支持通过行业模版关联脱敏算法，自动生成脱敏规则，降低系统维护工作量。	

			脱敏规则： 1.自动发现增量的敏感数据并根据模版来生成相对应的规则，实现无人值守； 2.支持视图查询脱敏； 3.支持表复制脱敏，自动对复制表增加规则脱敏，防止脱敏绕过； 4.支持应用脱敏防写入，并提供开关选择，可有效防止更新把查询到脱敏的数据写回数据库覆盖原有数据； 5.支持设置脱敏白名单对指定规则脱敏，满足脱敏例外需求。	
			扩展规则： 1.支持将高危SQL语句请求替换成其他自定义SQL语句，限制特定用户/IP/时间下的访问权限； 2.支持对SQL语句内的关键字进行搜索并替换成新关键字，如表名、列名等，灵活控制用户访问行为； 3.支持对删除数据库、truncate等高危语句的阻断。	
			应用级用户权限控制： 支持应用系统用户级别的识别和判断，实现细粒度用户权限访问控制。	
		规格要求	标准2U上架专用设备，冗余电源；提供千兆电口≥4、万兆光口（含万兆多模光模块）≥2、管理口≥2，硬盘≥2*2T，硬盘扩展槽≥8；最大脱敏列数≥60，最大脱敏能力≥15K单元格/秒，最大并发数≥4000；默认数据库实例授权≥20，最大扩展实例≥30，大数据集群扩展≥2。	
			系统易用性： 1.基于B/S方式，采用HTTPS方式远程WEB安全管理，中文操作界面，无需安装管理客户端； 2.支持安全模式（HTTPS）和常规模式（HTTP）切换，满足多样部署场景需求。	
			业务高效性：支持通过数据资产状态仪表盘功能实现脱敏业务的快速部署配置，支持自动发现用户环境中增量的敏感数据并根据模版来生成相对应的脱敏规则，实现无人值守，提升工作效率。	
			部署方式： 1.支持反向代理部署方式，脱敏系统无需在数据源安装任何代理程序，针对数据库环境仅通过JDBC数据接口配置 2.支持旁路引流的部署方式，无需修改客户端的连接IP即可实现动态脱敏效果，支持通过策略路由快速恢复业务，反向代理方式与旁路引流方式可自由切换。	
			提供1年维保服务及软件升级。	

4.1.1.2.2.10静态数据脱敏系统

表3-13 静态数据脱敏系统技术要求

序号	产品名称	技术要求	数量
		系统安全： 1.支持会话超时配置，超过指定时长未操作，会自动退出当前会话； 2.支持验证码登陆，避免暴力破解； 3.支持根据密码失败次数、锁定时长设定密码失败锁定策略； 4.支持密码使用期限配置，避免长时间不更改密码导致的严重安全问题。	

1	静态数据脱敏系统	功能要求	敏感识别： 1.脱敏系统内置大量敏感字段识别规则，可以自动发现以下敏感字段：中文姓名、中文地址、身份证、组织机构名称、电子邮件、IPV4地址、IPV6地址、统一资源定位系统地址、电话号码、手机号码、银行卡号、工商注册号、组织机构代码、税务登记号、统一信用代码、军官证号码、车牌号、中国护照、港澳居民来往内地通行证、外国人永久居住证、邮政编码、证件号码混合、姓名和组织机构名称混合； 2.支持自定义敏感信息发现规则，发现规则支持基于正则表达式、关键字匹配和字段名匹配三种方式；支持自定义混合敏感数据发现规则； 3.支持白名单功能，对于符合条件的数据不识别为敏感数据； 4.可对识别出的敏感字段做梳理，梳理后的敏感字段支持excel 模板导出与导入。	1套
			脱敏规则： 1.脱敏系统内置中文姓名脱敏规则、中文地址脱敏规则、身份证脱敏规则、组织机构名称脱敏规则、电子邮件脱敏规则、IPV4地址脱敏规则、IPV6地址脱敏规则、统一资源定位系统地址脱敏规则、电话号码脱敏规则、手机号码脱敏规则、银行卡号脱敏规则、工商注册号脱敏规则、组织机构代码脱敏规则、税务登记号脱敏规则、统一信用代码脱敏规则、军官证号码脱敏规则、车牌号脱敏规则、中国护照脱敏规则、港澳居民来往内地通行证脱敏规则、外国人永久居住证脱敏规则、邮政编码脱敏规则、随机替换规则、置空规则、日期随机脱敏规则、数值随机脱敏规则； 2.支持自定义脱敏规则，可以基于长度、分隔符进行拆分成任意数量的数据分段，每个数据分段均可以自由配置脱敏算法，由各分段的不同算法，组合成脱敏规则。	
			脱敏模式： 1.支持数据库脱敏到数据库； 2.支持数据库脱敏到文本文件； 3.支持文本文件脱敏到文本文件； 4.支持文本文件脱敏到数据库； 5.支持各类数据库之间的异构脱敏，无需操作人员进行任何额外操作，全自动化将字段类型进行映射和转换； 6.支持对自动映射和转换的字段类型进行手动修改； 7.支持增量脱敏。	
			数据子集：在脱敏配置中，可以通过配置SQL语句，实现数据表部分数据抽取脱敏，即可以实现抽取行数限定，也可以实现抽取部分字段的限定。	

			脱敏特性： 1.数据库脱敏系统保证脱敏前后的数据特征不变，脱敏后数据保持原业务属性，如中文姓名脱敏后的数据为中文姓名、手机号脱敏后的数据也为手机号、身份证号码脱敏后的数据也为身份号码等，且保证脱敏后的数据通过校验； 2.保证脱敏结果的唯一性，保持数据脱敏后的关联关系 数据库脱敏系统具备复合数据处理能力，能脱敏一列中混合了多种敏感类型，例如：对证件列含有身份证号码、组织机构代码等复合数据进行脱敏； 3.数据库脱敏系统具备复杂数据处理能力，能脱敏在一个单元格内由多段敏感数据组合的数据，例如：姓名/手机号码这种复杂数据的脱敏； 4.在执行数据库脱敏任务时，除了要将数据脱敏至目标库以外，还会同步触发器、函数、存储过程、视图、序列、type、type body、package、package body、队列表、索引、主外键。
			支持类型： 1.支持人大金仓、达梦（DM）、高斯等主流数据库的脱敏； 2.支持TXT、CSV、DEL等文件的脱敏。
			脱敏模板： 支持数据库和文件脱敏模板，用户创建任务，上传模板即可完成敏感数据确认、脱敏算法选择等，便于快捷对数据库和文件进行脱敏。
			任务计划： 1.系统支持脱敏任务直接单次运行功能； 2.系统支持定时、定期自动执行脱敏任务的功能； 3.系统支持周期时间内重复执行脱敏任务的功能。
			脱敏审批： 系统具备审批模块,系统中操作员可以创建脱敏任务,但需要管理员审批后脱敏任务才可执行。
			权限管理： 1.支持对不同用户配置不同权限； 2.对用户可设置数据源对应关系，分配不同的数据源给不同的用户。用户无法对未授权的数据源执行脱敏任务； 3.数据源支持细粒度授权，数据库授权到schema级别，文件服务器授权到目录级别。
			系统监控：支持自身系统性能监控，能够对CPU、内存、磁盘状态进行实时的展现。
			数据安全： 支持数据不落地脱敏，脱敏系统不留存脱敏前后的数据。
		规格要求	采用B/S架构，全中文web管理，默认包括： 敏感数据识别模块、敏感数据脱敏模块、脱敏规则管理模块、审批管理模块、日志管理模块。默认支持不少于20个生产数据库实例授权。
			提供1年维保服务及软件升级服务。

表3-14 应用日志审计技术要求

序号	产品名称	技术要求		数量
1	应用日志审计系统	功能要求	可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。	1套
			支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。	
			内置不少于5000条解析规则，支持对收集的不少于5000种设备类型日志进行解析（标准化、归一化），解析维度不少于200种，解析规则支持定制扩展；	
			▲支持通过网络资产、安全知识库、弱点库（风险库）三个维度分析事件是否存在威胁，并形成关联事件；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
			▲支持通过部署采集插件，以监测被审计主机的CPU、内存、磁盘等关键指标的使用率以及网络流量等信息；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
			支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警；	
			资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。	
		性能要求	平均处理能力（每秒日志解析能力EPS）：≥4000 EPS。	
			峰值处理能力（每秒日志解析能力EPS）：≥5000 EPS。	
		规格要求	支持审计不少于500个日志源。	
			提供1年维保服务及软件升级服务。	

4.1.1.2.2.12数据库审计

表3-15 数据库审计技术要求

序号	产品名称	技术要求		数量
			审计协议： 支持人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase)等。	
			审计能力与效果： 1.系统应内置规则集，对数据库DML、DCL、DDL等语句及FTP、Telnet等协议中的命令进行归类，便于用户定制； ▲2.支持关键对象和操作审计，具体如下：支持对数据的访问时间、源目IP、源目端口、源目MAC、资源账号、数据库名、规则名称、表名、命令、SQL语句、连接方式、客户端程序名、客户端用户、SQL执行结果等的审计；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	

1	数据库审计系统	功能要求	基于场景的审计： 1.针对异常场景自动生成审计结果，免配置，异常场景包含且不限于：异常账号访问审计、数据库异常审计、同账号多IP登陆、同账号上下班时间操作统计、访问时长异常审计、操作全审计等。▲2.支持异常场景分析，具体如下：支持对数据库用户变更检测、疑似暴力破解、疑似撞库攻击等场景的异常分析；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	1套
			事件查询统计与报表： 1.支持按时间、级别、源\目的IP、协议名、源\目的MAC、源\目的端口为条件进行查询； 2.具有CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能。	
			响应方式： 记录审计事件、记录会话数据、忽略、界面告警、Syslog告警、SNMP trap告警、邮件告警、短信告警。	
			安全联动： 1.支持与APT检测产品的联动，对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件； 2.支持与Web应用防火墙（WAF）的联动，可对WAF上报的应用系统攻击实现场景还原展示。	
		性能要求	审计分体机数据中心： 入库速度≥80000条/秒，日处理事件数≥10亿条。	
			审计分体机旁路引擎： 系统吞吐量≥4Gbps，可审计流量≥1400Mbps。	
		规格要求	审计分体机数据中心： 标准2U设备，冗余电源，配置≥1个管理口，≥1个HA口，≥6个千兆电口，≥4个千兆SFP插槽，≥2个万兆SFP+插槽，≥2个硬盘扩展插槽，≥2个USB口，≥2*4T硬盘容量，配置不少于200个DB授权。	
			审计分体机旁路引擎： 标准2U设备，冗余电源，配置≥1个管理口，≥1个HA口，≥6个千兆电口，≥4个千兆SFP插槽，≥2个万兆SFP+插槽，≥2个扩展插槽，≥2个USB口。	
			提供1年维保服务及软件升级。	

4.1.1.2.2.13万兆数据安全交换系统

序号	产品名称	技术要求		数量
1	万兆数据安全交换系统	功能要求	支持基于网闸隔离的文件、数据库、接口等数据交换方式。	2套
			支持文件交换功能。支持通过ftp、http等方式进行文件单向、双向交换。支持文件交换完整性。	
			具备数据库交换功能。支持Gbase（南大通用）、KingBase（人大金仓）、DM7（达梦）等数据库的同步交换。	
			支持接口化同步调用，可有效保障数据交换的实时性。支持以Web Service接口、REST API方式接收数据进行内外数据交换。支持基于XML报文的请求服务，实现内外系统的实时数据交换。	
			支持kafka数据交换，适配视频云、大数据平台等大规模消息交换业务。	
			支持文件常规检查功能，可对交换的文件进行基于正则表达式的文件名及后缀名（扩展名）检查。	
			支持基于文件特征的文件类型检查功能，即基于文件内容特征检查文件类型，当启用文件特征过滤功能时，文件特征符合策略的文件，将触发相应处理措施。	
			支持恶意代码扫描功能，可对文件进行病毒、木马等恶意代码检测。	
			▲支持文件内容关键字检查功能，可检查文件内容是否包含指定关键字；支持XML报文附件检查功能，可对XML报文的附件解析后进行病毒、木马等恶意代码检测。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
		性能要求	文件交换：≥250MByte/s，数据库交换：≥10000条/s，接口调用：≥10000个/s。	
		规格要求	万兆数据安全交换系统，由内外安全交换系统和隔离网闸等3台设备组成。	
			内外安全交换系统要求为2U标准机架式机箱，冗余电源；	
			网络接口：≥2个千兆电口，≥2个万兆SFP+插槽(含2个万兆多模SFP+模块)	
			隔离网闸要求为2U标准机架式机箱；冗余电源；	
			系统架构：采用2+1系统架构即内网单元+外网单元+FPGA专用隔离硬件。不能采用网线等形式直通。	
			网络接口：内网≥6个10/100/1000M BASE-TX接口，≥2个万兆SFP+插槽(含2个万兆多模SFP+模块)；外网≥6个10/100/1000M BASE-TX接口，≥2个万兆SFP+插槽(含2个万兆多模SFP+模块)。	
			提供1年维保服务及软件升级服务。	

4.1.1.2.2.14系统运维安全管控系统

表3-16 系统运维安全管控系统技术要求

序号	产品名称	技术要求		数量
1	系统运维安全 管控系统	功能要求	支持用户管理，包括添加、删除、启用、禁用、移动、修改功能。	1套
			支持资源管理功能，包括添加、删除、启用、禁用、移动、修改功能。	
			支持资源制定不同改密分组，执行周期性、手动改密操作。	
			支持主机、安全设备、网络设备、应用系统等运维管控。	
			支持SSH协议服务端启用强加密算法，提升SSH协议安全性。	
			支持用户以手机号码或邮箱地址作为用户身份登录。	
			支持扫描本地运维工具并进行配置保存，简化运维人员使用配置过程。	
			支持根据需求对特殊指令操作进行二次审批功能，运维人员操作过程中触发命令策略，需要得到审批员的审批后才能继续执行后续操作。	
			▲支持受控授权的应用发布，具体如下：支持通过应用发布开启运维屏幕水印，且运维方本地无法篡改水印内容；支持对操作记录进行视频回放时，水印能够显示运维用户；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
			支持管理员下发工单，授权运维人员有权限在指定时间内访问指定的资源。	
		规格要求	系统管理： 1.采用HTTPS方式远程安全管理，系统自身HTTPS 证书签名支持高强度SHA256算法； 2.支持实时监控CPU、内存、磁盘的使用情况。	
			性能要求	
			字符会话≥800路，图形会话并发≥200路，配置≥100个资源授权。	
			标准机架式设备，专用硬件平台和安全操作系统，配置≥6个千兆电口，≥2个万兆多模光口，1T硬盘。	
			支持在IPV4,IPV6, IPV4与IPV6网络环境下部署。	
			提供1年维保服务及软件升级。	

4.1.1.2.2.15数据库运维管控系统

表3-17 数据库运维管控系统技术要求

序号	产品名称	技术要求		数量
			组件功能： 1.应用服务器子系统提供统一登录界面、单点认证、主从账号管理、审计日志管理、系统管理等，实现对运维操作的集中管理、访问控制、单点登录以及操作审计等功能； 2.发布服务器子系统提供应用发布模块、应用代填模块、应用窗口推送模块，资源列表管理模块等； 3.数据管控服务器子系统提供数据集中管理、个人目录管理、数据下载审批、数据备份等；实现数据上传/下载的审批审计，提供个人工作目录及数据上传/下载控制及审批审计，提供个人数据远程编辑及流转。	
			数据存储:数据存储分为文档存储和数据存储。	

1	数据库运维 管控系统	功能要求	支持协议审计: 1.支持Gbase（南大通用）、KingBase（人大金仓）、DM7（达梦）等数据库类型; 3.支持通过应用发布进行协议审计，记录命令详情，包括字符协议和数据库协议等，审计回放支持协议回放和图形回放。	1套
			文档集中管控: 1.支持独立的存储空间集中存放用户文件，无须文件同; 2.支持用户上传、下载文档审批、免审批功能; 3.文件夹的创建、重命名、删除、复制; 4.文件的分发、重命名、复制、删除; 5.支持对所有用户文件的产生、流转均以日志方式记录，并备份记录; 6.支持通过发布的工具在线查看文件夹中文件。	
			防拷贝:支持禁止设备操作端直接拷贝文件或字符到本地终端。	
			金库模式: 1.支持加密、非加密字符协议的命令授权和复核（支持Telnet/SSH、FTP/SFTP协议）; 2.数据库金库：支持SQL语句的授权和复核（支持Oracle、DB2数据库）; 3.预授权金库模式(用户登录后台系统资源时预先进行金库审批流程）; 4.实时金库模式(用户登录后台系统资源后，触发金库敏感信息时进行金库审批流程)。	
			身份认证及访问授权: 1.支持账号+口令认内部AD域认证、数字证书认证、手机二次认证；内置令牌管理员、口令管理员角色; 2.使用人员不必知道服务器帐号及密码，无需进行二次登录认证；支持用户多次登录失败自动锁定账号。	
			访问控制及告警: 1.按口令用户、保护主机、匹配规则等内容或按访问授权策略设定安全事件规则，支持指令黑白名单; 2.支持对违规或高危操作的指令（黑名单）进行告警、忽略处理、自动阻断或审批。	
			主账号密码管理: 允许运维管理根据需要制定多个不同的密码策略，并将这些密码策略赋予不同的管理对象，包括系统管理员、运维人员。	
			从账号密码管理: 1.按设备、系统帐号、计划开始时间、改密周期等信息配置改密计划，到期自动执行; 2.自动改密，支持自动修改数据库内置自身账号密码; 3.支持自动改密结果发送到指定改密计划的管理员邮箱。	
			操作行为记录: 1.针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计，记录会话时间、命令执行时间、会话协议、服务端IP、服务器端口、客户端IP、客户端端口、操作命令、信息、运维用户帐号、资源账号等信息; 2.针对RDP、VNC等图形终端操作的连接情况进行记录及审计，记录会话时间、会话协议、服务端IP、服务器端口、客户端IP、客户端端口、运维用户帐号、资源账号等信息; 3.会话协议回放空闲时间过滤，应用发布图像操作回放支持操作空闲过滤。	

		设备安全性： 1.支持通信加密、探互相认证，防止欺骗、防止日志/策略在传输过程中被篡改； 2.内核重新编译，不采用通用的TCP/IP堆栈，避免通用TCP/IP堆栈的缺陷导致的安全漏洞； 3.具有Watchdog功能，确保系统的长期稳定运行。
		系统管理： 支持实时监控审计系统CPU、内存、磁盘的使用情况；
		扩展接口： 1.资源&用户信息同步接口基于RESTFul或视图两种方式，从第三方系统获取用户身份信息、资源信息、认证信息、权限信息等； 2.审计传输接口基于syslog协议的实时接口，基于FTP定期上传日志的非实时接口，向日志采集平台提供审计日志； 3.应用调用接口采用WebService接口方式，为第三方提供调用应用发布工具连接资源； 4.SSO单点登录接口提供Webservice认证实现单点登录接口。
	规格要求	支持不少于200个资产接入服务。
		提供1年维保服务及软件升级服务。

4.1.1.2.2.16攻击欺骗诱捕系统

表3-18 攻击欺骗诱捕系统技术要求

序号	产品名称	技术要求	数量
		伪装能力： 1.支持伪装数据库伪装能力，包括人大金仓、达梦等常用关系型数据库及大数据数据库； 2.支持工控网络仿真能力，包括 modbus、s7comm的伪装，可用于专用系统； 3.支持常用运维服务的伪装，包括：ssh/telnet/VNC； 4.支持GitHub互联网诱饵投放,迷惑攻击者，诱骗攻击者进入仿真系统，记录后续所有操作，产生告警； 5.支持线下制作仿真系统，包括中高交互应用类、低交互协议类、Web类。	
		日志记录与追踪能力： 1.支持记录捕获的所有攻击行为，包括且不限于时间、蜜罐名称、蜜罐类型、源IP、攻击类型、源端口、目标IP、目标端口等信息等； 2.支持记录入侵全过程，如以命令形式展示用户的命令操作记录，如FTP、SSH等蜜罐； 3.支持样本捕获功能，可通过各种方式上传到蜜罐主机的可疑样本文件，提供恶意样本提供下载接口； 4.支持攻击者信息追溯，追溯到攻击者真实外网IP、地理位置、个人账号等内容，包括百度账号、微博账号、CSDN账号等个人账号信息； 5.支持基于IP的白名单识别，对于可信主机可加入白名单。	
	功能要求		

1	攻击欺骗诱捕系统	展示能力： 1.支持监控数据展示，以图形化和结构化方式展示蜜罐监控数据，以时间、入侵事件、入侵源IP、目标IP月统计方式呈现； 2.支持对蜜罐数据进行统计分析，包括网络、事件、样本等，以时间或蜜罐机为单位生成报表； 3.支持全局统计，展示在一定时间内受到的入侵事件，并可以导出报告，支持Html、PDF格式中的报表导出； 4.支持web界面管理配置，可对管理平台、节点和监控获取的数据进行管理，支持平台和节点的资源使用情况，包括CPU、内存、硬盘等。	2台
		系统管理： 1.支持三权分立，至少包含管理员、操作员、审计员三种角色，支持自身操作日志的记录，录用户名、登陆IP、操作类型、操作内容、操作时间等日志信息； 2.支持系统离线升级，提供升级接口； 3.支持系统平台的资源管理与监控，包括CPU、内存、连接数，磁盘使用情况，各网卡的上下行流量等，以便发现异常行为； 4.支持用户静态密码的复杂性设置，登录失败次数设置，登录失败超过配置的次数后限制登陆，提供IP限制登录功能。	
		第三方接口： 1.支持告警数据syslog、邮件方式推送监控平台； 2.集群统一升级，多台蜜罐统一部署的环境下支持版本统一升级； 3.支持集群模式部署。	
		硬件规格： 标准2U机架式设备，提供≥6个千兆电口，≥4个千兆SFP插槽，≥2个万兆SFP+插槽，≥1个接口扩展槽位（支持万兆接口扩展），≥2个USB口，内存≥32GB，HDD硬盘≥2TB，仿真系统≥15。 部署方式：旁路部署，支持不同蜜罐投放至不同网段。 提供1年维保服务及软件升级服务。	

4.1.1.2.2.17网站云安全监测系统

表3-19 网站云安全监测系统技术要求

序号	产品名称	技术要求		数量
1	网站云安全监测系统	功能要求	网站漏洞扫描： 可检测SQL注入、XSS跨站脚本、目录遍历、脚本源码泄露、目录浏览、可能的敏感文件等常见漏洞。检测内容覆盖WASC分类的≥25种Web应用漏洞和OWASP TOP10 网站漏洞。 挂马监测： 支持对多种挂马方式（如Iframe、CSS、JS、Body挂马）等进行检测。 可用性监测： 1.通过ping、get 和http等方法，分别从域名可用性、网站服务可用性和网站程序可用性进行监测； 2.可对多个监测点同时进行监测，监测频率可以根据需求进行更改； 3.可对IPV6地址进行监测； 4.自动发送邮件和手机短信告警。 页面篡改监测： 1.基于快照定义的网页变更监控； 2.可对当前网页和快照的文本和图片对比，不同的文本区域应使用不同颜色标出； 3.支持网页快照使用正则表达式过滤生成； 4.手动和爬虫两种任务生成方式， 爬取链接数量可根据网站大小自行选择； 5.支持页面框架对比、页面相似度、图片MD5值等技术，能够智能的检测出网站页面出现的变化； 6.支持对网站中常见正常变更的过滤，如过滤网页计数器、日历、访问人数统计等，形成通用白名单策略，减少告警误报； 7.监测频率可以根据需求进行更改，可自动发送邮件告警。 网站域名解析监测： 1.支持配置多个DNS服务器，对各DNS服务器的解析结果进行对比及时发现域名劫持等问题； 2.支持对解析到的异常DNS地址进行邮件报警； 3.监测频率可以根据需求进行更改。 敏感内容监测： 1.判断网站是否存在恶意发布的违法、反动、色情等敏感信息，并进行定位和告警； 2.采用多模式字符串匹配技术，使用内置敏感词库及自定义敏感词对相关网页进行深度解析； 3.监测频率可以根据需求进行更改，自动发送邮件告警。 安全通告： 1.通过邮件进行及时报警，每周、每月发送监测报告； 2.支持发送PDF、word、EXCEL格式的安全通告文档。 服务： 提供1年维保服务及软件升级。	1套

表3-20 安全运营支撑平台技术要求

序号	产品名称	技术要求		数量
		规格要求	产品形态： 支持中标麒麟、统信、银河麒麟等操作系统部署，产品应具备hadoop等大数据组件技术，支持分部署部署，支持后期横向扩展。	
			采集种类： 1.支持内置≥180余种的数据源类型开箱即用，默认可接入各类硬件设备和应用系统，包含但不限于主机、防火墙、IPS/IDS、WAF、网络设备、安全设备、数据库、应用系统、中间件、存储、设备、虚拟化设备、机房设备等多种设备和系统的日志接入方式； 2.支持 AWS数据通过S3直接采集。	
			采集方式：支持业内通用标准数据获取方式，获取方式不少于15种，包括 Syslog、SFTP、文件、Kafka、HDFS、主机终端Agent、人大金仓、SNMP、Netflow、WMI、ES、AWS等。	
		数据标准管理： 1.支持数据标准的属性配置，系统内置不低于1000余种属性满足绝大多数场景需要，例如威胁类型、DOS攻击、威胁特征、登录类型。同时可以在线配置扩展新的属性字段形成新的标准，包括IP型、整型、长整型、浮点数、时间、字符和枚举等类型； 2.支持通过选择映射的方式由定义的属性字段组成生成各种对象来归类管理，避免手动直接编辑导致的错误配置，满足各种分析层面的需要，包括日志对象（威胁、事件等）、计算机对象（主机、流量、文件、进程、驱动、登录等）、安全设备对象（防火墙、沙箱、蜜罐、情报等）、协议对象（TCP、SMB、DHCP、FTP、HTTP、DNS等）。		
			数据过滤： 支持图形化数据过滤配置，包括删除字段、字段裁剪、删除整条数据、json字段提取、格式化成json对象或数组、字段拆分等过滤方法。支持设置数据源的置信度，有助于评估该类日志的可信程度，包括：高、中和低三个级别。	
			数据解析： 1.系统预置不少于1000条范式化解析规则，支持解析规则的导入导出。所有解析操作支持可视化的配置界面； 2.支持选中日志中任意字符串，自动生成正则解析语句，减少人为错误并提升解析速度； 3.支持字段解析的自动化智能推荐，根据该日志数据的特点自动推荐匹配优先的对象类型，同时在字段映射时自动推荐靠前的字段类型。系统用不同的颜色提示推荐字段的匹配程度，减少人为选择的错误并提高效率。	

数据存储: 1.支持基于ElasticSearch深度优化的分布式索引, 存储热数据同时用于实时的分布式搜索和数据分析引擎, 实现TB级数据秒级响应。支持多集群部署, 灵活横向扩展; 2.支持Hadoop分布式文件系统(HDFS)技术, 能提供高吞吐量的数据访问以适应在大规模数据集上的应用, 作为温数据角色来存储需要长期保存的数据。支持高度优化索引管理Parquet、ORC等文件来达到文件压缩比为15:1。
关联场景和方式: 1.关联分析系统的模型配置支持图形化配置和管理, 有助于根据场景运营, 支持修改所有预置关联分析规则, 支持新建关联分析规则, 关联分析规则修改、新建, 不接受后台代码化实现方式; 支持不少于60种, 700条规则的安全检测分析场景的開箱即用, 场景包括: 扫描探测类、主机异常类、异常通信类、运维监控告警类、中间人攻击类、Web攻击类、账号异常类、拒绝服务类、邮件攻击类等; 2.支持关联规则多级 and、or、not 等逻辑操作符, 属性字段支持IP、字符串、数字、时间等多种类型, 属性字段操作支持网段包含、字符串匹配、情报匹配、正则表达式匹配等多种操作符。支持把前一个关联分析结果作为内部事件为作为后一个关联规则的输入进行多级(数量无限制)关联分析的嵌套, 以支持复杂的关联分析; 3.支持关联规则根据数据标准进行规则编写的自动化推荐, 系统根据事件类型自动推荐其所属的对象, 并且会自动判断规则内容是否与该对象匹配, 如果发生错误会用红色标出并警告; 4.支持关联规则在配置时评估该策略运行所使用的资源情况, 在线显示该规则的性能指标, 分为优、良、差多个级别。
时序关联分析: 支持A事件后发生B事件, 事件A发生后关联产生B事件, 如检测到webshell连接后疑似通过mysql提权。事件前置条件是webshell连接成功, 连接成功后通过mysql有提权操作, 这两件事30分钟内先后发生。
检索分析: 支持同比分析算子, 根据历史的同周期数据进行对比并判定偏差度来发现异常线索。支持通过同比昨天、上周、上个月及自定义周期的方式来计算, 根据统计变化率(如同比增长10%, 增长20%-40%等)或变化的绝对值(如登录次数同比增长5次)来进行同比分析。
攻击聚合: 1.支持自动化威胁猎捕模型, 可在线编写脚本语言算法模型模拟分析人员溯源取证的过程, 基于告警事件为入口触发条件的威胁场景自动溯源分析, 向前、向后自动抽取若干分钟、小时和天为单位的数据, 结合时间、过滤条件关联, 多层逻辑嵌套、自动聚合分析包括日志、流量、告警等内容, 聚合跨阶段展示整个威胁事件; 2.支持将告警按照整个事件的攻击链、攻击方向聚合及攻击时间轴排序, 整合为一个事件的完整攻击链阶段。并根据聚合事件的安全评分模型化动态评估威胁数值, 模型维度包括不限于告警数量、告警等级、攻击阶段、威胁情报。

1	安全运营支撑平台	聚合检测库： 1.内置不少于15种聚合事件威胁场景，如Tomcat遭受暴力破解攻击后被上传webshell，并发起了445端口扫描、FTP账号被暴力破解成功后数据遭到窃取、内网主机遭受远程漏洞攻击后连接矿池、UAC提权并驻留并发现Powershell系列攻击等； 2.系统模块内置横向移动聚合模型，通过以进程执行哈希传递攻击告警、黑客脚本工具invoke_Psexec行为和哈希传递登录行为为入口，自动化溯源聚合多源告警和行为的关联关系，检测出哈希传递技术手段的登录事件突破边界横向移动并还原攻击者上下文操作的安全事件； 3.系统模块内置信息统计聚合模型，通过聚合主机访问行为、命令执行安全告警、服务器短时间内频繁执行信息收集命令告警、运行代理工具告警等多源数据进行自动化提取和校验，检测出主机遭受ssh暴力破解后主机层面出现异常命令操作行为，爆破成功并驻留。	1套
		安全事件监测和分析： 1.支持通过key-value模式或类SQL模式进行安全事件检索； 2.支持自动根据严重等级、事件分类、处置状态和确认状态等不同维度的各种详细分类进行统计，通过简单勾选检索出关注的事件，无需手动输入检索条件； 3.支持把安全事件相关的网络攻击关系和终端进程演变过程融合为一张攻击链路图，通过静态观察和动态回放来分析网络行为、终端行为的攻击过程，为失陷过程分析提供形象化分析手段。根据不同对象（如资产、IP、域名）进行图中元素区分，同时支持点击后关联展示对应上下文； 4.支持安全事件将所有相关告警的处置建议进行统一汇总和展示，对每个告警有对应的分析内容和处置建议，提供兼容ATT&CK并且新增扩展的缓解建议和检测建议。	
		资产管理和监测： 1.支持资产与相关漏洞、威胁的关联后评估风险，并以资产维度展现资产相关的漏洞与威胁，资产风险评估包括资产信息（包括IP、端口、协议、服务名、操作系统版本、责任人等）、资产的脆弱性情况、资产受到的威胁攻击情况等多维度信息。展开可监测资产的历史IP与MAC地址、关联的脆弱性、关联的安全事件、关联的告警。安全事件和告警可直接下钻到对应的安全事件分析和告警列表进行拓展分析和溯源取证； 2.支持资产实体的行为画像，画像的行为包括但不限于本机发起网络事件、访问本机的网络事件、本机发起的登录行为、进程创建行为、注入行为、注册表操作、敏感文件操作、计划任务操作等，行为分类随着当前实体触发的异常行为自动扩展。每种分类中可以描绘维度根据该类行为特点而边，例如注册表操作包括事件名称、注册表地址、注册表值、注册表名等，而注入行为包括事件名称、进程MD5、进程路径、目的进程路径、数量等。	
功能要求			

技战术分析：

- 1.支持知识图谱技战术热力图，支持通过颜色深浅来代表该技术的攻击强度。以及支持点击攻击技术，查看详情，包括不限于子技术、技术描述，相关安全事件等；
- 2.支持Mitre ATT&CK之外扩展出具备技战术总结。

自定义监测和分析：

- 1.支持自定义各类图表并进行权限控制，支持公开、不公开。支持自定义仪表盘配置，根据需要添加不同的监控组件，自定义选择过滤条件和过滤条件组的监控组件添加、修改和删除。支持同时组合多种展示图形，如柱状图、饼图、面积图、趋势图、表格、统计、同比、环比、百分比、复合计算统计、上传图片、外部图片、外部网页等，可配置排序方法、TOP数量、数据时间跨度。
- 2.仪表盘的图形位置和大小支持自由拖拽，所见即所得；
- 3.支持从仪表盘下钻至具体事件、告警、资产等并且可直接配置下钻选项，支持跳转到自定义的其他仪表盘，实现仪表的嵌套来满足分析需要。支持仪表直接调用SOAR预案来快速处置，支持仪表的内容通过点击快速变为过滤条件。

综合检索：

- 1.支持对日志、告警、事件、漏洞、资产、风险、预案进行检索分析；
- 2.支持添加结构化语言过滤条件和过滤条件组对内容进行查询，支持查询条件支持 **and**、**or**、**not** 等多重逻辑操作组合，支持等于、不等于、大于、小于、存在、不存在、属于（内置安全信息）、网段包含、字符串匹配、正则表达式匹配等多种操作符；
- 3.支持检索一键切换BI分析，通过可视化BI图表自定义展示与分析，图表展示包括直方图、折线图、面积图、饼图、表格、统计值、同比、环比等多种类型，多维度快速展现数据的价值，在分析过程中支持设定周期自动刷新；
- 4.支持仪表盘和报表模板对BI分析结果的直接引用，BI分析所用的查询条件和BI图例一起保存和发布。

专家检索：

支持在主查询语句中嵌套子查询语句，多查询语句的管道连接，以支持复杂场景，管道支持任意级别，支持对字符串、数字、时间等类型的参数进行常见函数调用,支持函数超过1000个；支持平均值、计数、去重计数、最大值、最小值、差值、求和等统计聚合函数；支持**search**、**where**、**bucket**、**stats**、**sort**、**join**、**fields**、**head**、**top**、**format**、**append**等搜索命令。

报表管理： 1.支持从原始日志与流量、安全设备告警、平台关联告警以及安全事件输出多个层面自动呈现统计数据。支持对概况、事件、IP地址、端口、服务、事件严重程度、攻击种类、用户等数据进行统计。报表内容支持自定义编辑，直接引用图标、文本、链接、图片、宏变量、嵌套报表、外部网页等元素； 2.报告中数据支持统计查询与过滤条件满足与、或、非、In、Not In、exist字符串匹配、正则匹配等基础组合。支持报表图形化结果展示包括但不限于柱状图、饼图、面积图、趋势图、表格、统计、同比、环比、百分比、复合统计等。支持周期性（每日、每周、每月）自动生成报表并通过邮件发送、下载、导出等方式获取； 3.支持导出WORD/PDF/HTML/EXCEL等格式，报告可指定人员进行分享。
威胁攻击态势： 支持不少于6种态势感知大屏宏观审视全貌。将具体的安全事件以3D到2D的形式展示出攻击源和攻击目标，通过地理位置直观掌握宏观攻击概况。通过攻击源国家的排名了解攻击者，对攻击致命、严重、警告和提醒事件一周的变化趋势掌握全局危险数量，通过受害IP、攻击阶段和最近24小时攻击趋势了解攻击的严重程度和攻击面，最严重事件的排名指引关注危害最高的威胁。
安全成果态势： 需要通过该态势掌握各类安全事件的检测和产生分类，直观了解威胁情况。包含从原始日志到安全告警、安全事件多个层级描述安全建设实现的效果，体现整体安全事件的收敛和运营工作量以阶梯递进的图形化方式展现日志数量、告警数量到安全事件数量一步步减少的聚合演变，了解通过运营达到的效果。安全事件级包含总体事件条数和高危事件数量，并根据不同事件类型（如Web攻击、主机异常、恶意程序）通过条形比例的方式进行展示，同时列出高危安全事件的TOP10排名及其处置状态，便于直观监测。对于网络整体的告警量、日志量通过环形图的方式展示不同数据源的比例，以及排名前五的数据源，从宏观上了解网络内安全设备的贡献率。
运行监控态势： 支持监控系统全集群的运行状况包括但不限于CPU使用率、内存使用率、磁盘使用率，支持运行状态异常的节点给出告警提示，支持监控接入各数据源的数据上报情况，支持实时展示整体日志采集速率、告警生成速率，以及整体安全信息的入库速率。
威胁情报态势： 支持展现威胁情报总量、更新情况，当前系统中威胁情报的分类、数量。以及当前系统威胁情报告警情况，高频命中的情报IOC、攻击团伙\家族等。
系统配置： 支持指定告警通知属性配置，定义告警通知方式为短信、邮件和命令行扩展（短信、命令行需根据实际情况定制），定义通知对象分组和策略组，如配置事件等级为“高危”通知管理员01，告警类型为“Webshell”通知管理员02，资产为“办公网”的通知管理员03。告警通知策略可灵活运用不同的安全模型。

			数据备份：支持对配置信息根据内容选择后进行导出、导入，对于在线更新的模型可以选择保留用户修改的数据，同时对于更新后不满意可选择过往的版本进行一键倒回，方便运维管理。
			运维监测： 1.支持监测各节点、各模块运行状态。 支持详细记录资源使用情况、模块运行情况、软件访问情况等信息。监控最近5分钟的使用情况，如CPU使用率、内存使用率、磁盘剩余容量、网络I/O、磁盘I/O等数据； 2.支持记录平台运行情况，包含不限于日志接收量、实时处理EPS、数据采集EPS情况。
			全局数据关联分析： 1.支持跨数据中心关联分析，能自动将规则拆分下推到所有数据中心并提取所需全局字段，产生全局数据关联分析告警，无需日志数据传输交互，无需日志数据上传至某一节点进行汇总分析； 2.支持区分全局规则和局部规则，全局规则由上级节点统一发布生效，下级节点不可修改； 3.局部关联规则仅本地生效，下级节点看不到全局规则和本地规则以外的其他规则。
			用户管理： 支持用户功能分权和数据分权管理，功能分权可以将平台的每个功能进行独立指定不可见、只读和读写权限；数据分权能与组织机构进行映射，通过类SQL结构化检索语言定义日志、告警的字段、字段组合进行数据分权范围。
			安全管理： 支持管理员口令更换周期策略，指定更换天数，支持双因子登录（Email 或短信），认证码通过邮件发送，提高账号访问安全性。支持设置可登录到系统的IP白名单，支持指定某账号开启加密数据可见权限，防止无权限账号看到敏感数据，支持指定某账号开启对内置数据存储和数据源可见权限。
规格要求		日志处理性能：日志处理性能EPS≥2万；支持集群部署，节点数不少于2个。	
		提供1年威胁情报升级服务、维保服务及软件升级服务。	

4.1.1.2.2.19主机漏洞扫描系统

表3-21 主机漏洞扫描系统技术要求

序号	产品名称	技术要求		数量
1	主机漏洞扫描系统	功能要求	支持软件虚拟化部署，采用容器技术，便于在不同基础设施中快速部署。	1套
			支持Web应用和主机服务扫描；具备Web应用被动扫描能力，通过代理监听Web应用运行状态，自动识别和发现漏洞。	
			支持IPv4和IPv6环境的部署和扫描。	
			Web扫描任务中，支持配置参数包括最大并发连接数、超时时间、爬虫类型、爬虫爬取深度、爬虫路径等。	
			主机扫描任务中：支持配置参数包括：并发主机数、主机存活探测强度（超时等待时长、最小/最大重试次数）、端口扫描强度（超时等待时长、最小/最大重试次数）等。	
			支持针对弱口令扫描功能，包含不限于AMQP、DB2、FTP、IMAP、JBoss、MySQL、MongoDB、PostgreSQL、phpMyAdmin、Redis、RDP、RTSP、SSH、SNMP、Telnet、SMTP、SMB、VNC、WebLogic、WebBasic、Zabbix等协议。	
			支持对漏洞扫描能力，包含且不限于麒麟、统信UOS、银河麒麟（Kylin）操作系统，人大金仓、达梦、南大通用、神通、PingCAP、Informix数据库，金蝶、中创、东方通中间件等。	
			系统内置漏洞库数量不少于22万。	
			系统内置“扫描插件”数量不少于800项，实现验证式漏洞发现能力。	
			针对0day或突发漏洞，可生成应急策略，快速定位并进行风险监测。	
			系统内置扫描插件支持对网络安全产品（如终端安全、日志中心、行为感知、网络监控设备）、业务应用系统（如OA、计费管理系统）在HW中暴露的0Day漏洞检测验证。	
			支持漏洞自定义POC，能够根据0Day或用户需求，在管理页面提供编写漏洞检测脚本功能。系统内置《自定义检测脚本编写指南》与示例代码，供用户学习使用自定义POC功能。	
			支持登录录制，使用“登录录制工具”可录制用户在浏览器的操作，上传生成的yaml可在扫描时自动重放登录操作。	
			系统自带盲打平台，不需额外部署，可实现对存储型XSS、SSRF等无回显漏洞的验证。	
			支持多管理账户、多角色管理，灵活设置角色权限，符合三权分立原则。	
			支持多种格式报告导出（HTML、Word、excel）。	
			漏洞按照风险等级分为严重、高危、中危和低危。	
		规格要求	最大并发扫描任务数≥10；	
			提供1年全模块特征库升级服务、维保服务及软件升级服务。	
			支持引擎节点扩展，实现对单任务并发量的扩展。	

4.1.1.2.2.20云密码资源池管理平台

表3-22 云密码资源池管理平台技术要求

序号	产品名称	技术要求		数量
1	云密码资源池管理平台	功能要求	设备管理： 1.支持云密码机的注册、增删、配置等管理功能； 2.支持虚拟密码机的增删、启停、配置、分组等操作； 3.支持B/S和命令界面对设备进行管理。	1套
			系统工作台能够展示虚拟化设备和实体设备的占比、设备分配情况、各种类型设备占比等信息。	
			审计可查看平台管理员从登录到登出之间的所有操作，并在记录审计日志时使用管理员Key对审计记录进行了签名防止抵赖。	
			支持设置用户端和运维端。	

4.1.1.2.2.21密钥管理系统

表3-23 密钥管理系统技术要求

序号	产品名称	技术要求		数量
1	密钥管理系统	功能要求	提供对称密钥和非对称密钥的全生命周期管理，包括密钥生成、存储、导入/导出、备份/恢复、更新、销毁和删除等操作。	1套
			提供应用管理、设备管理、租户管理、日志管理和监控管理等内容。	
			支持密钥策略的细粒度管理，支持对单个密钥设置加密、解密和密钥获取控制策略，对每个密钥操作设置访问时间等操作。	
			支持对系统中所有的关键操作均记录日志，并且会对操作进行基于密码技术的完整性校验，可对系统中所有的日志进行查询，并且验证其有效性。	
		性能要求	密钥数量≥50万个，SM1加解密速率≥100Mbps，SM2签名速率≥2400Tps，SM2验证速率≥1400Tps，客户端并发数量≥500个，KMIP创建密钥速率≥160TPS，KMIP获取密钥速率≥400TPS。	

4.1.1.2.2.22云服务器密码机

表3-24 云服务器密码机技术要求

序号	产品名称	技术要求		数量
1	云服务器密码机	功能要求	支持SM2、SM3、SM4等国密算法。	2台
			支持密钥生成、数据加密解密、消息鉴别码产生和验证、数据摘要产生和验证、物理随机数产生等密码运算功能。	
			支持对虚拟密码机内的每种密码运算单独设置运算速度。	
			具备基于SR-IOV环境下，密码虚拟机资源并发有序调度的能力，保障资源互不挤占、按序调度。	
		性能要求	单台设备可虚拟≥64台虚拟设备。	
			并发连接数≥50000、SM1加解密≥800Mbps、SM4加解密≥800Mbps、SM3≥800Mbps、SM2密钥对生成≥22000对/秒、SM2签名≥50000次/秒、SM2验证≥40000次/秒、SM2加密≥12000次/秒、SM2解密≥14000次/秒。	

4.1.1.2.2.23应用安全网关

表3-25 应用安全网关技术要求

序号	产品名称	技术要求		数量
1	应用安全网关	功能要求	算法支持：1.支持SM2、SM3、SM4算法。 ▲2.支持后量子密码算法，具备证书请求、密钥及证书导入、证书管理功能，基于后量子算法实现SSL通信，保障传输安全。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	2台
			▲适配性：适配鲲鹏CPU平台，且可保障流量分发（SLB）、SSL、流量编排等主要功能稳定运行。（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）	
			SSL功能： 1.支持SSL拦截白名单，只允许通过指定的域名访问特定的SSL服务； 2.支持客户端证书过滤功能； 3.支持SSL DDOS防御； 4.支持客户端IP透传； 5.支持当用户证书发生过期、废除、损坏等情况，可自定义友好的引导页面告知用户； 6.内置硬件SSL加速卡，支持HSTS、SSLI、SDNS等功能,满足ATS策略要求。	
			支持SSL侦听功能。	
			服务器负载均衡功能：支持L4、L7服务器负载均衡。	
			支持Tuxedo协议、RADIUS协议的负载均衡。	
			支持QoS Diameter负载均衡策略。	
			HTTP功能：支持TCP Option传递客户端IP。支持将客户端证书的DN一键逆序插入至HTTP Header、统一资源定位系统、Cookie当中。	
			高可用功能：支持SSI单系统映像。	
			基于CPU、内存占用率、SSL加速卡状态进行条件筛选进行主备机切换或设备重启。	
		性能要求	负载性能：每秒新建连接数≥10000 TPS，并发会话数≥160000 TPS，最大吞吐≥30Gbps。	
			SSL性能：并发会话数≥20000TPS,并发连接数≥10000 TPS，最大吞吐≥12Gbps。	

4.1.1.2.2.24签名验签服务系统

表3-26 签名验签服务系统技术要求

序号	产品名称	技术要求		数量
1	签名验签服务系统	功能要求	多应用支持：支持不同应用的证书及对应密钥的生成及存储。	1套
			多信任域支持：支持配置不同的证书信任域，证书验证策略支持配置不验证、根证书、CRL等多种验证策略。	
			数字签名/验证：支持基于SM2算法的签名/验证。	
			带签名的数字信封加密和解密：支持基于SM2算法的带签名的数字信封加密、解密功能。	

4.1.1.2.2.25文件加密系统

表3-27 文件加密系统技术要求

序号	产品名称	技术要求		数量
1	文件加密系统	功能要求	加解密接口： 1.支持加解密接口，通过集成SDK实现平台功能； 2.扩展数据加密、解密功能，可对前端页面请求的数据进行安全处理。	1套
			准入控制管理：支持加解密接口的使用管控，只有预设定好且被允许接入的前提下，在调用接口时才会被允许接入到服务器，以保障接口的安全使用。	
			数据文件加解密：由于重要的文档数量远远小于普通文档，为了方便使用，可设置系统为手动加密方式，用户有针对性的挑选重要的文档进行加密保护，在此并不影响普通文档使用。	
			权限控制：支持对每个用户进行详细的权限控制管理，具体控制的权限包括：阅读、编辑、复制、打印、截屏等。管理员可以根据业务需求制订相应的权限策略。不同部门用户可以通过文档授权功能进行文档共享与交流或者直接允许部门间可以文件相互流通，不做访问控制。	
			应用策略管理:根据不同的应用环境，支持定义只有授权的程序才可读取加密数据文件的正确内容，同时可根据实际需求定义授权程序使用数据的管控的程度，从而实现自动加密、手动加密等力度轻重不一的梯度式数据防护效果。	
			用户角色管理:提供4种角色，分别是普通用户、特权人、普通管理员、控制台管理员。其中普通用户可提升为普通管理员、特权人，用户可具多重身份方便用户使用，反之可以灵活的根据需要权限进行降级。	
			事件审批管理:系统可对客户端提出的各种操作申请进行审批，申请类型包括解密、离线。而事件的审批员可设置多级审批人，逐级审批，也可指定特定审批员审批。针对特殊情况，还支持无需审批的特权人，但系统会以日志形式记录特权人或审批员的操作。	
			行为日志管理:所有操作、审批、解密等等都将会被记录，如果你的计算机因出差离线，连上采购人网络后也将会自动上传日志。以及管理员对后台的操作策略的更改，每一个终端对加密文件的操作都会有日记记录，从而给采购人以详细的日志或报表查询，便于事后审查。	
		性能要求	加解密速率不小于35MB/s。	
			可支持通过中国信息安全测评中心安全可靠测评的64位图形界面操作系统。	
			支持Docker、Tomcat等常见容器部署。	
			支持国密算法。	

4.1.1.2.2.26 SSL服务器证书

表3-28 SSL服务器证书技术要求

序号	产品名称	技术要求		数量
1	SSL服务器证书	功能要求	1.提供域名身份的真实性验证； 2.根证书-CA证书链密钥长度4096位 - 2048位； 3.加密强度支持使用256位加密，可兼容支持128位； 4.支持单向、双向SSL协议；支持国密SM2算法。	2张

4.1.1.2.2.27 RSA服务器证书

表3-29 RSA服务器证书技术要求

序号	产品名称	技术要求		数量
1	RSA服务器证书	功能要求	1.提供域名身份的真实性验证；根证书-CA证书链密钥长度4096位-2048位； 2.加密强度支持使用256位加密，可兼容支持128位； 3.支持单向、双向SSL协议； 4.支持RSA算法。	2张

4.1.1.2.3服务成果

服务方案，应包括人员安排、质量保障计划、故障响应措施等内容；提交季度巡检报告、故障和问题处理记录（如发生）；防御能力监测报告、安全资源池授权升级单等。

4.1.1.3全厅REDIS租赁服务

4.1.1.3.1服务内容

租赁全厅自然资源云专区267G的REDIS数据库服务，保障业务系统的支撑平台稳定运行。

支撑业务系统清单如下：

表3-30 全厅REDIS租赁服务支撑业务系统清单

序号	系统名称	ID/实例名称	架构版本
1	海洋生态保护修复数据应用	10059/海洋生态保护修复数据应用	Redis 5.0标准版
2	海洋资源资产数据应用	10058/海洋资源资产数据应用	Redis 4.0标准版
3	广东省国土资源测绘院-协同调查子系统	10057/广东省国土资源测绘院-协同调查子系统	Redis 4.0标准版
4	田长制子系统	10055/田长制子系统	Redis 5.0集群版
5	门户子系统	10050/crs-10050	Redis 4.0标准版
6	不动产登记系统	10049/crs-10049	Redis 5.0标准版
7	互联网+应用服务	10048/crs-10048	Redis 5.0标准版
8	综合感知服务系统	10047/crs-10047	Redis 4.0标准版
9	自然资源和不动产登记综合应用-不动产交换区	10046/crs-10046	Redis 5.0集群版
10	自然资源和不动产登记综合应用-不动产外网区	10045/crs-10045	Redis 5.0集群版
11	广东省土地整治与生态修复监测监管系统	10043/crs-10043	Redis 5.0标准版
12	省自然资源厅地质灾害数据综合管理系统-地灾防治服务项目	10042/crs-10042	Redis 5.0标准版
13	广东省测绘地理信息监管与服务系统	10040/crs-10040	Redis 5.0标准版
14	卫星遥感影像管理与服务	10039/crs-10039	Redis 5.0标准版
15	省自然资源厅地质灾害数据综合管理系统-勘查钻孔数据采集系统	10037/crs-10037	Redis 4.0标准版
16	常态化监测数据管理主题-数据中台	10036/crs-10036	Redis 5.0集群版
17	海洋数据管理应用系统	10035/crs-10035	Redis 4.0标准版
18	广东省地质资料数据库管理系统	10034/crs-10034	Redis 5.0标准版
19	自然资源与不动产登记信息管理基础平台	10033/crs-10033	Redis 5.0标准版
20	海洋经济应用子系统	10032/crs-10032	Redis 5.0标准版
21	广东省自然资源市场与开发利用监测监管子系统	10031/crs-10031	Redis 5.0标准版
22	遥感影像智能识别基础框架	10030/crs-10030	Redis 5.0标准版

23	智慧自然资源快速制图服务系统	10029/prd_n_redis_ggdtfw_kszt	Redis 5.0标准版
24	省市县多级地图服务系统	10028/prd_n_redis_ggdtfw_sxxdj	Redis 5.0标准版
25	广东省矿产资源储量监测管理服务系统	10027/crs-10027	Redis 5.0标准版
26	海岛应用专题子系统	10026/prd_n_redis_jdyy	Redis 5.0标准版
27	海砂开采智能监管系统	10025/prd_n_redis_hyyy_hskc	Redis 5.0标准版
28	自然资源调查检测辅助综合管理	10024/prd_n_redis_dcjcfzzhgl_jw	Redis 5.0标准版
29	广东省自然资源厅测绘产品质量监督检验管理系统	10023/prd_n_redis_zljd_nfsm	Redis 5.0标准版
30	广东省海域使用管理技术审查子系统	10022/prd_n_redis_hyyy_jssc	Redis 5.0标准版
31	全民所有自然资源资产信息管理监管	10021/prd_n_redis_qmzcxx_gd	Redis 5.0标准版
32	决策参阅	10020/prd_n_redis_jccy_sg	Redis 5.0集群版
33	常态化监测感知管理主题	10019/prd_n_redis_cthjcgzgl_sg	Redis 5.0标准版
34	国土空间规划配置与协同服务	10018/prd_n_redis_gtkjghpzyxt_ja	Redis 5.0标准版
35	数据中台	10017/prd_n_redis_sjzt_sg	Redis 5.0集群版
36	时空数据管理与服务	10016/prd_n_redis_sktpgl	Redis 5.0标准版
37	用途管制综合应用	10013/prd_n_redis_ytgzzhyy_sh	Redis 4.0标准版
38	赋能中心	10012/prd_n_redis_fnzx_cxs	Redis 5.0标准版
39		10011/test_n_redis_fnzx_sg	Redis 5.0标准版
40		10010/prd_n_redis_fnzx_sg	Redis 5.0标准版
41		10009/test_n_redis_fnzx_ht	Redis 5.0标准版
42		10008/prd_n_redis_fnzx_ht	Redis 5.0标准版

4.1.1.3.1服务成果

提供12个月的租赁服务；提交服务方案，应包括人员安排、质量保障计划、故障响应措施等内容；提交月度巡检报告、故障和问题处理记录（如发生）等。

4.1.1.4 CA设备及证书租赁服务

4.1.1.4.1服务内容

广东省自然资源一体化平台门户、自然资源和不动产登记综合应用等重要系统，需每年续订数字证书服务，包括210个证书的授权服务以及认证服务端的授权服务，维持厅机关及下属单位用户CA密钥的有效可用。

4.1.1.4.2服务成果

服务期内提供满足数量和服务要求的CA证书服务；故障和问题处理记录（如发生）等，服务期结束提供项目服务总结报告。

4.1.1.5安全产品特征库升级授权租赁服务

4.1.1.5.1服务内容

为现有8台安全设备（2台360网神防火墙、2台网御Power V6000-F83G2-HD、2台网御Power V6000-F7310、1台网御入侵检测系统TD3000-GS3500、1台网御高级持续性威胁检测与管理系统）提供1年的特征库升级。

安全产品特征库授权按下表内容提供：

表3-31 安全特征库清单

序号	产品	特征库种类
1	360网神防火墙NSG5000-TG65M-Q	应用识别库、统一资源定位系统分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务
2	360网神防火墙NSG5000-TG65M-Q	应用识别库、统一资源定位系统分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务
3	网御星云Power V6000-F83G2-HD万兆防火墙	防病毒特征库
		入侵防御特征库
4	网御星云Power V6000-F83G2-HD万兆防火墙	防病毒特征库
		入侵防御特征库
5	网御星云Power V6000-F7310	防病毒特征库
		入侵防御特征库
		上网行为管理特征库
6	网御星云Power V6000-F7310	防病毒特征库
		入侵防御特征库
		上网行为管理特征库
7	网御星云TD3000-GS3500	入侵检测特征库
8	网御高级持续性威胁检测与管理系统	入侵检测特征库

4.1.1.5.2服务成果

服务期的有效升级授权；升级实施报告。

4.1.1.6安全基础设施租赁服务

4.1.1.6.1服务内容

提供2台防火墙部署于省自然资源厅政务外网边界，为省自然资源厅政务外网公共平面、业务网网络平面、不动产登记虚拟专网网络平面提供安全防护。提供2台万兆防火墙部署于省国土资源技术中心，为省国土资源技术中心不动产登记虚拟专网网络平面、业务网网络平面提供安全防护。提供1套终端安全管理系统部署于省国土资源技术中心，为外来技术服务人员使用电子政务外网提供入网、用网安全管控。

表3-33 安全基础设施租赁服务内容

序号	服务项	服务内容
1	防火墙	租赁2台防火墙，部署于省自然资源厅政务外网边界，为省自然资源厅政务外网公共平面、业务网网络平面、不动产登记虚拟专网网络平面提供安全防护。
2	万兆防火墙	租赁2台万兆防火墙，为省国土资源技术中心不动产登记虚拟专网网络平面、业务网网络平面提供安全防护。
3	终端安全管理系统	租赁1套终端管理系统（200个授权点），加强外来技术服务人员使用广东省电子政务外网的安全管控。

4.1.1.6.2服务成果

- 1.服务期内提供满足数量和服务要求的安全设备；
- 2.安全设备实施报告；
- 3.故障和问题处理记录（如发生）等。

4.2软件开发服务

4.2.1成品软件租赁服务（许可）服务

4.2.1.1广东省自然资源一体化管理与服务平台（国土空间基础信息平台）云盘

厅政务办公需要提供文档存储协作管理、系统集成对接实现在线文档能力、文档格式转换能力，为省自然资源厅提供平台支撑服务能力，实现政务业务系统文档在线办公全生命周期管理，实现政务数据资源能够充分整合、开放共享、高效利用。基于云文档，按照自然资源业务需求，提供电子文件的统一使用管理和使用。

延续租赁云盘的在线编辑、在线预览、格式批量处理、云文档等功能，本期项目拟延续租赁云盘一年。

4.2.1.1.1云盘

延续租赁云盘，性能需充分考虑自然资源厅实际使用情况，云盘服务需为广东省自然资源厅提供 ≥ 600 用户授权，以满足不同部门的存储需求。云盘部署采用高可用性架构，即使在硬件故障、软件故障或网络故障的情况下，也能保障服务的持续运行。

云盘服务的高并发支持 ≥ 1000 个文档同时在线访问， ≥ 50 用户并发数、 $\geq 2T$ 云盘容量，以满足高效协作和数据共享的需求。

4.2.1.1.1.1在线编辑

在线编辑服务为提供高效的文档处理方式，集成Office客户端的主要功能，以web页面的方式进行功能和文档内容的呈现，业务系统可以将此能力嵌入到任何对文档进行在线编辑或协同编辑的场景中，无需任何插件。提供可随时随地的编辑能力，提供基于文档的协同能力，并且可由业务系统自定义编辑权限、版本管理、文档水印。

4.2.1.1.1.2在线预览

文档在线预览提供完全按照排版结果形成的文字所属行段页锚点位置的相对位置进行切分渲染输出html显示内容，保证文档的内容显示效果符合不跑版。

1、预览分页传输

在线预览内容查看时运用数据分页渲染输出的技术，针对不同文档格式分别应用不同的数据分块计算和渲染规则，形成可查阅的分页的数据，客户端按查看进度实时分段管理数据缓存，加快内容显示速度。

2、文档预转机制

在提升预览查看速度上，文档预览采用预转机制，根据上传来源、时间、使用频率等不同维度，配置高效的预转队列和分布式节点的执行策略。

4.2.1.1.1.3格式批量处理

文档格式转换提供支持批量将文字、表格、演示转换为对应格式的任意一种，如：文字支持将doc转换为docx、wpt或txt等，表格支持将xls转换为csv、xlsx、et、xlsm等，演示支持将ppt转换为pptx、pot、potx等。同时支持将以上格式转换为PDF、OFD和PNG。

1、内容处理：文档清稿、文档水印。可同时调用，也可以单独使用。支持在文字、图片和PDF添加离线水印。支持对文字的内容进行清稿（接受修订）。

2、书签替换：在模板中使用书签，帮助使用者定位需要填充的内容位置，通过定位到的书签位置工作人员可以对文档的内容进行自定义填充。可用于插入红头（图片）、填充具体文字或将某个文档的内容填充到具体章节。

4.2.1.1.1.4云文档

4.2.1.1.1.4.1文档协作管理

4.2.1.1.1.4.1.1文档权限

云盘可对用户在团队文档的操作权限进行严格的管控，针对用户以及团队设置文档级的阅读、编辑、复制粘贴、导出、另存、打印等精细化的权限。只有具有权限的用户才能对文档进行操作，没有权限的用户无法进行任何操作。

对于拥有文档授权权限的用户和文档安全管理员可以将权限授予给其他用户、部门或用户组，保证拥有文档分发权限。构建文档的全生命周期保护，实现文档应用中的细粒度安全。

4.2.1.1.1.4.1.2团队管理

在云盘中主要分为部门团队和普通团队。

部门团队根据组织架构自动生成。若组织架构人员有变动，会自动同步增删相关人员到团队成员列表里，也可以手动添加其他部门人员到部

门团队里，对团队内部成员进行个性化管理。

普通团队是可自由创建的虚拟团队，团队拥有者或管理员可自由添加团队成员，解决短期、临时组织任务的文件共享、协同办公的问题。

团队管理主要用于对团队成员以及对团队文档的权限管控。团队管理员通过对成员和文档进行多层次的管控，管理员全面掌控、保障团队文档资产，提高团队协作，减少因文档管理不当造成的信息泄露或数据丢失。团队成员也能快速定位属于自己权限范围内的文件，快速融合，高效协作。

4.2.1.1.1.4.1.3成员管理

在云盘中，根据所拥有的团队管理权限的区别，可将团队成员分为团队拥有者、团队管理员、团队成员。团队管理权限包含团队管理、权限管理以及文件（夹）管理。

团队拥有者拥有团队管理的所有权限。团队管理员拥有除转让团队、删除团队以外所有的团队管理权限。团队成员默认拥有除回收站外的基本团队文件权限，无团队管理、权限管理权限。

对团队成员所拥有的权限进行精细化、规范化管理，使团队中各类文档使用秩序井然，管控松紧得当，有效保证文档安全。

4.2.1.1.1.4.1.4权限设置

团队管理中的权限设置主要包含两类，团队管理权限设置和文件（夹）权限设置。

团队管理权限包括检索团队、指定拥有者、批量指定部门团队拥有者、批量导入团队成员、空间分配、查看成员、恢复团队、删除团队等操作。为保障团队内部文档的安全性，云文档对文档的操作权限进行严格的管控，团队拥有者和管理员可以对文件（夹）进行权限设置，包括但不限于只读、编辑、下载等权限，针对特定人员可增加自定义权限。

4.2.1.1.1.4.1.5全文检索

云盘支持对办公文档全格式的支持和分布式检索引擎索引，云文档支持快速和准确的全文内容检索。文档上传到云文档后，可通过文档内容提取工具将文档中所有的内容，包括各子文档内容、隐藏内容，导入到分布式索引引擎中，建立索引仓库。索引仓库的数据支持多维度，满足各种场景组合的全文检索需求。

4.2.1.1.1.4.1.6文档标签

云盘通过文档标签实现文档的分类索引和管理，根据用户的分类策略，建立文档的标签，同时利用分布式搜索引擎的能力，实现快速查找文档。文档的标签类型支持机构强制标记和用户自定义两种，可实现机构和用户个人有专属的分类数据，实现不同层面的文档管理需求。

4.2.1.1.1.4.1.7文档分享

云盘支持只要一个链接就可以分享。文件分享时可以进行多样权限设置，选择公开分享或指定范围分享，设置链接失效，限制查看/编辑/下载/另存/打印等权限；分享后，可以取消或关闭链接，保障安全稳妥。

4.2.1.1.1.4.1.8协同编辑

当一份文档需要多人共同编辑，例如：拟稿、会稿等多人协同编辑 word、PPT 等场景，可通过云盘实现多人、多终端同步在线协作编辑，修改版本实时保存，协作记录一目了然。云盘支持编辑锁控制，实现高效编辑的同时，灵活控制协作模式。

4.2.1.1.1.4.1.9版本管理

云端的每一个在线文档都会有历史版本体系，且都是通过对唯一文档 ID 维系不同版本集，进而对每个独立的文档 ID 维护一个版本序号关系表，这样两个维度的关系管理可保证文档在大量存储下仍然可以准确匹配访问，且可满足随时按需恢复特定版本，保证数据不错乱。

通过历史版本可以查看文档修订记录、更新的内容以及更新人，支持恢复历史版本，避免文档在流转过程中丢失、损坏的风险。

4.2.1.1.1.4.1.10权限模板

可配置权限模板，用于一组权限的授予，不必每次都单个权限授予。权限模板可通过模板名称、模板编号、模板描述、维护人姓名、模板类型等条件进行单个条件或组合条件的搜索。管理员还可通过新建、编辑、删除完成权限模板的管理。

4.2.1.1.1.5表单收集

云盘提供表单应用作为安全专业的数据收集工具，可快速收集信息及汇总数据。支持手机电脑多端使用。可用于机构信息收集汇总、问卷、投票等场景，通过自定义的字段和配置，发送给用户填写，避免一张表格多人查阅，保护敏感隐私信息，快捷收集到的用户信息直接汇总至表格并自动生成报表。协作收集的数据自动汇总存储，便于后续筛选复用和导出。

4.2.1.1.1.6文档安全

4.2.1.1.1.6.1安全团队

云盘支持创建安全团队。当文档被上传到云盘安全团队时，通过安全文档的加密模块实现云上加密，拥有安全文档有对应权限，才能对文档进行预览、编辑。同时，安全团队提供权限设置管理，可对团队内的文档进行权限模板设置，实现文件精细粒度的权限管控。

4.2.1.1.1.6.2加解密文档

在保证一文档一密钥的同时，客户端和服务端对文档信息、密钥等数据进行双重加密。支持加解密机制，无需通过驱动、hook 等技术手段，从而增加系统稳定性。此外，加密流程深度整合到云盘的处理文档过程，加快文档数据的处理效率并且无明文落地。还可由第三方提供加密算法，扩展程序已规范化的接口接入 WPS 安全系统。

4.2.1.1.1.6.3细粒度权限管理

打开安全文档和对文档进行操作都会受到权限限制，拥有阅读权限的用户在登录后通过服务器鉴权才可以打开安全文档进行浏览，其他编辑、复制、打印、另存、离线、授权操作都会受到相应的权限管控，没有权限的用户无法进行该操作。需支持Windows、iOS、Android 系统的客户端支持进行权限控制。

4.2.1.1.1.7管理后台

4.2.1.1.1.7.1机构通讯录

机构创建者或管理员可以通过云盘管理后台对使用云文档的人员进行集中管理，进行日常的增加、修改、禁用、查询账号；同时支持同步固定的组织架构，支持账号同步、第三方业务系统账号同步、手动添加/批量导入账号。

4.2.1.1.1.7.2空间管理

管理后台统一提供空间管理功能，支持管理者全局分配各个业务、团队、人员的空间使用量，合理利用存储空间，平衡分配，实现空间价值最大化。

4.2.1.1.1.7.3数据统计

在管理后台可全局查看云端使用情况的统计信息，包括用户量、文档量、空间量等的多维度统计数据。

4.2.1.1.1.7.4日志审计

用户机构内用户对安全文档进行的创建、阅读、编辑、复制、另存、打印、授权操作都会被服务器记录下来。管理员可以通过管理后台定期对安全文档进行审计工作，通过日志时间、文档名称、操作者名称等条件进行筛选，某一个文档被某个用户做过何种操作都可以随时查出来，还能批量导出日志。

同样，系统记录的管理员在后台进行的外发收件人维护、权限模板维护、导出日志、同步用户等操作行为信息，管理员也可以定期对安全文档进行审计工作。

4.2.1.1.1.7.5角色管理

管理后台可以设置多个管理员角色，默认支持常规管理员角色，如：超级管理员、系统管理员、部门管理员、策略管理员、日志管理员，同时还可以按需要添加自定义角色。可针对不同角色管理员设置不同资源的管理权限。

4.2.1.1.1.8开放平台

4.2.1.1.1.8.1文档赋能

云盘开放平台向开发者提供面向业务提供多种方式的文档云存储与文档协作的集成能力。

对接方式一：对接业务系统可选择将文档上传至云文档进行统一存储管理,同时云文档开放平台提供文档协同编辑能力支撑。业务系统应用实现权限验证、目录管理、文档分享和协同权限设置。

对接方式二：业务系统自身实现文件存储、目录、版本管理能力的同时也需实现用户登录验证、文档分享和多人协同权限设置。

4.2.1.1.2文件转换迁移系统

4.2.1.1.2.1多格式转版

系统可采用后处理方式实现大批量文档的异步转换，支持转换指定文件夹所有文件，主要用于历史文件批量转换为国标OFD格式和多业务系统的批量转换需求，将Office、WPS、PDF、图片、网页、Visio、TXT、CEB、CEBX、SEP、AIP、PS、二扫、CAJ、XPS、EML、CAD等格式文件转换为OFD版式文件，也可将OFD文件转换为PDF文件、CEB文件和图片文件,实现OFD格式与PDF、CEB及图片格式的互转功能。

在格式转换过程中，还可设置相关内容属性：

支持设置图片的页面宽高、压缩质量、DPI、合并长图等参数。

支持网页转成OFD时可添加页码、页眉页脚等内容。

支持在流式文件转成OFD版式文件时，可保留流式文件中的修订内容、批注内容等文档元素，保持相关内容活性。

具体支持的格式清单如下：

表3-1 文件转换迁移系统支持的格式清单

序号	分类	子类	支持格式
1	流转版	word转ofd	doc、docx、wps、wpt、rtf、dot、dotx、docm、dotm、uot、uof、txt、xml
2		excel转ofd	et、ett、xls、xlsx、xlt、xlsm、csv、xltx、dif、uos、uof、dbf
3		ppt转ofd	dps、dpt、ppt、pptx、pot、pps、pptm、potx、potm、ppsx、ppsm、uop、uof
4	版式互转	pdf转ofd	pdf
5		ofd转pdf	ofd
6		ceb转ofd	ceb
7		ofd转ceb	ofd
8		sep转ofd	sep、gd、gw
9		ps转ofd	ps
10		s2转ofd	s72、s92、s10、s2
11		caj转ofd	caj
12		cebx转ofd	cebx
13		xps转ofd	xps
14		ofd转ofd-a	ofd
15		aip转ofd	aip
16	图片版式互转	image转ofd	bmp、jpg、jpeg、png、gif、tif、tiff
17		image转pdf	
18		ofd转image	
19		pdf转image	
20	其他	html转ofd	html、htm、mht、mhtml
21		html转pdf	html、htm、mht、mhtml
22		visio转ofd	vsd、vsdx
23		cad转ofd	dwg、dwt、dwf、dxf
24		eml转ofd	eml、msg

4.2.1.1.2.2套版转换

实现XML文件或结构化文件套用指定OFD模板转换生成为特定显示格式和版面的OFD文件，满足业务系统中各种套打功能和报表的版式化需求。

4.2.1.1.2.3版式加工

提供OFD版式文件二次加工功能，可在转换的同时同步处理文档元数据、字体嵌入、页面、水印、二维码、签名/签章、附件等。可按需生成安全OFD文件，实现文档加密和权限控制功能

4.2.1.1.2.4文档属性

可对文档元数据、视图模式、字体等属性进行设置。

1、文档元数据

支持在OFD文件中添加、删除文档元数据信息，可在电子公文中添加符合《党政机关电子公文元数据规范》（GB/T 33480-2016）的公文元数据，在证照文件中添加符合《电子证照 元数据规范》（GB/T 36903-2018）的证照元数据。支持用户自定义元数据。

2、视图模式

支持设置视图模式属性，包括页面布局、页面模式、缩放倍率、窗口控件（显示/隐藏）等，首次打开文档后可按属性进行页面显示，再次打开文档时则参照阅读器的默认设置进行页面显示。此功能方便快速定位阅读页面。

3、内容处理

支持对OFD文档内容进行处理，可在文档指定区域添加掩膜，实现对区域内容进行遮盖处理，保护敏感信息。

可为OFD文档添加页码信息，可设置页码位置、字体、大小、颜色等属性；可根据业务推送的目录信息，转换为OFD文档的目录页；支持添加背景图、红头和版记。

支持内容脱密处理，包括签章脱密（黑章）、红头置黑、图片置灰。

4、字体嵌入

支持在OFD文档中嵌入字体，可自动识别并嵌入文档已使用字体，也可嵌入指定字体，从而保证各种环境下的文档内容呈现效果一致，避免因缺少字体字库发生字体跑版等现象的发生。

4.2.1.1.2.5 文档处理

可对OFD文档内容进行加工处理，包括页面处理、组合拆分、内容处理、文档水印、签名/签章、附件处理等，满足不同场景的应用需求。

支持文档脱密功能，使得签章变为黑色、红头置黑、图片置灰等。支持文档注释迁移、添加标引。

1、页面处理

支持OFD文档页面处理功能，包括删除页面、插入页面、交换页面、旋转页面、裁剪页面等，使得文档内容更加符合业务需求、更加规范。

2、组合拆分

支持将多个文档按要求组合成一个OFD或PDF文件，其中OFD文件合成时创建文档大纲。可将一个OFD或PDF文件按要求拆分为多个OFD、PDF文件或图片文件。提供将DOC、DOCX、WPS文件按照大纲进行拆分功能。

可组合的文档格式包括Office、WPS、OFD、PDF、图片等，对多个不同格式的图片文件可指定组合后的页面宽度、分辨率和像素。

3、信息抽取

支持信息抽取功能，Word信息抽取可实现表格信息抽取、目录结构抽取、文档内标题抽取、文本内容抽取、图片信息抽取、指定模板流式文档内容抽取，可将文件属性键值对输出。OFD信息抽取可实现页码、元数据、验签结果、文档内容、签章信息、页面信息（页面宽高，旋转角度）、语义抽取。

4、文档水印

支持在OFD文档中添加文字水印和图片水印。文字水印属性包括指定添加的页码（奇偶页/连续页/指定页码）、位置、旋转角度、字体、颜色、字号、加粗、斜体、字距、行距、透明度、是否平铺等。

图片水印属性包括指定添加的页码（奇偶页/连续页/指定页码）、位置、旋转角度、透明度、是否平铺等。水印类型包括正文水印和注释水印两种，正文水印添加后不可删除，注释水印可以删除。支持在OFD文档的指定位置嵌入二维码图像。

5、签名/签章处理

支持与符合标准的数字签名/电子签章模块进行集成，实现在OFD文档上添加数字签名/电子签章，支持批量盖章、关键字盖章、归档章。支持对一个OFD文档添加多个电子签章，通过多版本技术保护文档内容。支持删除数字签名/电子签章功能。

6、附件处理

支持在OFD文档中添加、删除附件文件，也可对附件页面进行提取并放入正文后面，标记为附件。支持添加/删除XBRL文件。支持将附件转为OFD格式。

4.2.1.1.2.6 安全OFD

支持对OFD文档进行加密封装，可对文档进行加密和权限控制（包括编辑权限、打印权限、打印次数、复制权限、另存权限、注释权限、导出权限、签名权限、截屏权限等），可以设置文档阅读有效期，支持自动销毁。可对文档进行脱密处理，支持撤销签章信息。

4.2.1.1.2.7 高压压缩

系统内置高压缩算法，可对文字、图像进行高压压缩处理，被压缩后的文件可实现无损阅览和利用。

4.3运行维护服务

4.3.1基础设施运行维护服务

4.3.1.1基础设施运维服务

4.3.1.1.1服务内容

保障技术中心政务服务相关的存储、服务器、网络及安全设备，以及省厅机关政务办公网络设备的持续稳定运行。为自然资源政务办公，不动产登记信息管理，政务数据、时空数据和不动产登记数据等重要数据向云专区的交互提供支撑能力。运维对象为省自然资源厅及广东省国土资源技术中心共67台/套各类基础设施，包括网络、安全设备、运行环境保障设备等，服务内容包括例行巡检、日常维护、响应支持、故障处理等工作。

基础设施运维设备对象见下表：

表3-2 基础设施运维设备列表

序号	设备名称	规格型号	设备用途	单位	数量
1	精密空调	CANATAL GAU20	机房环境设备	台	2
2	精密空调	依米康SDA81U	机房环境设备	台	2
3	机房空调	大金FVY125DQV2CB	机房环境设备	套	1
4	机房空调	格力KF-50LW/(503581)CgD-	机房环境设备	台	1
5	机房空调	格力KF-120LW	机房环境设备	台	1
6	UPS系统	易事特EA66160含电池、配电柜	机房环境设备	套	1
7	机房气体消防系统	机房气体消防系统（含七氟丙烷气瓶）	机房环境设备	套	1
8	精密空调	科士达MT070DA	机房环境设备	台	2
9	路由器	华为AR2240	网络通信设备	台	1
10	核心交换机	华为S7706	网络通信设备	台	2
11	网络交换机	华为S5700-52P-LI	网络通信设备	台	12
12	网络交换机	华为S5720-36PC-EI-AC	网络通信设备	台	2
13	网络交换机	华为S5700-28P-LI	网络通信设备	台	3
14	VPN网关	网域PowerV-VPN-V6030	网络安全设备	台	1
15	堡垒机	网御 Leadsec-UDGAP-3500	网络安全设备	台	1
16	防火墙	网御Power_V6000-F3210	网络安全设备	套	1
17	防火墙	网御 Power_V6000-F3210	网络安全设备	台	1
18	IDS入侵检测系统	网御 TD3000-GS3500 IDS	网络安全设备	台	1
19	下一代防火墙	网御 Power_V6000-NF3210	网络安全设备	台	1
20	存储设备	HDS VSP G200	应用支撑及网络管理	台	1
21	存储设备	OceanStor 5500 V3	应用支撑及网络管理	台	1
22	万兆核心交换机	华为S12708	网络通信设备	台	2
23	网络交换机	S6720-54C-EI-48S-AC	网络通信设备	台	3
24	网络交换机	S5710-28C-PWR-E1-AC	网络通信设备	台	2
25	万兆防火墙	Power V6000-F83G2-HD万兆防火墙	网络安全设备	台	1
26	防火墙	360 网神 C5000-TF20P	网络安全设备	台	1
27	ATP网络安全检测系统	网御 APT3000-TD-M	网络安全设备	台	1
28	防火墙	Power V6000-F7310 防火墙	网络安全设备	台	1
29	VPN网关	Power-V-VPN-V2300-GD	网络安全设备	台	1
30	服务器	华为RH2288H V3 （管理节点）	应用支撑及网络管理	台	2
31	服务器	华为RH2288H V3 （应用节点）	应用支撑及网络管理	台	12
32	网络交换机	华为 S5700-28C-SI	网络通信设备	台	1
33	网络交换机	华为 S1728GWR-4P-AC	网络通信设备	台	1
合计					67

4.3.1.1.1.1例行巡检

要求对基础环境设施和硬件设备提供定期巡检服务。制定例行巡检方案，针对性能容量、可用性、可连续性、可管理性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现机房硬件设备的故障异常、设备告警、潜在问题、安全隐患等，并及时做出适当的处置，保障设备运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保设备能够7×24小时正常运行。巡检对象包括但不限于

于机房配电、UPS及蓄电池、机房空调、安防监控、网络设备、安全设备等。利用已有监控系统，按照标准规范要求进行监控操作，密切注意机房硬件设备情况。检查过程中同步记录运行数据，如若发现任何异常情况应及时进行登记，及时通知相关人员进行处理并跟进处理情况，每月形成巡检报告。

4.3.1.1.1.2日常维护

要求对硬件设备提供日常维护服务。制定日常维护方案，针对设备外观、标签标识、资产管理、业务保障等方面设定维护项，合理安排维护计划。在机房硬件设备的正常运行过程中，周期性开展常规维护保养工作，消除故障异常、设备告警、存在问题、安全隐患等，保障设备运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保设备能够7×24小时正常运行。按照标准规范对设备进行管理，定期形成设备使用记录。周期性保养维护工作每季度开展。

具体维护内容如下：

1.设备标识

定期检查设备的标识、外观和保洁情况。检查在用设备和线路等的标识和外观。若有标识残缺或外观破损时，及时进行修补。检查设备的积尘情况，确认是否需要对其进行除尘保洁。

2.设备检查和配置

定期检查设备硬件的运行情况和软件的配置情况，确保软硬件的配置能够匹配实际运行环境。根据实际运行环境的变化，对设备的软硬件配置进行调整，以适应新变化或新应用。

3.设备整理和测试

定期对网络设备和线路进行整理登记。根据实际需要，对线路进行通信质量测试，并根据测试结果调整设备和线路的使用分配。

4.设备台账管理

每年对设备进行盘点，设备台账包括：设备名称、设备型号、序列号、负责人、使用状态等；台账分类归档、内容完整、及时更新，并妥善保管；盘点设备发现丢失或损坏的，及时报告用户单位。

5.设备上架管理

对上架的设备进行标签编制及粘贴，标签内容包括：名称、IP地址、使用部门、用途等，由用户单位指定上架位置后实施；设备接入UPS之前需使用市电进行试开机。

6.设备运行和维护管理

对运维范围内的设备运行情况进行监控，动态掌握设备健康状态。对需要更新或维修的设备，应充分考虑业务连续性、安全性等条件后提供实施路线建议，经用户单位同意后，按用户单位管理流程执行。设备维修须填写《设备维护记录表》。

7.设备下架管理

用户单位有设备下架需求的，运维服务人员应协助用户进行设备下架工作。

4.3.1.1.1.3响应支持

响应支持服务，要求提供统一的服务热线电话，针对日常咨询、故障问题、专项任务、数据统计、服务投诉等服务请求进行统一登记，服务热线根据事件的性质、类别、等级进行判断，分派相关人员进行处理，并对事件处理全流程进行跟踪监督，确保服务请求得到及时的响应与处理。在服务热线电话发生故障情况下，提供便捷的备用联系渠道。响应支持工作按需常态化提供现场和远程技术支撑服务形式开展。远程响应时间要求小于2小时，现场服务到场时间要求小于24小时。

1.机房硬件设备日常咨询

协助进行硬件设备日常咨询的收集、整理、分析，跟踪日常咨询的解答情况。

2.机房硬件设备应用管理

协助提供表单配置、流程配置等机房硬件设备管理服务，调整服务器、存储、网络设备、安全设备各项设定。

3.信息化服务支持

提供日常硬件设备使用及信息化的支持服务。

4.硬件设备数据统计支持

提供例行、不定期和专题硬件设备的数据统计、提取服务。

5.备品备件服务

故障发生后在规定时间内不能恢复故障设备，提供相应备品替代使用，直至送修设备送回并正常使用为止。

6.基础环境日常咨询

协助进行设备运行环境日常咨询的收集、整理、分析，跟踪日常咨询的解答情况。

4.3.1.1.1.4故障处理

要求对广东省国土资源技术中心的硬件设备提供故障处理服务。当发生故障时，按照故障定级和处理流程，及时响应，快速抢通故障点，尽早恢复业务，将故障对业务所造成的负面影响降到最低。在处理完毕后清理现场,提供故障处理简报。故障处理按需常态化提供现场和远程技术支持服务形式开展。远程响应时间要求小于2小时，现场服务到场时间要求小于24小时。具体故障处理如下：

1. 当设备因老化、接触不足、容量不足、兼容性异常等出现运行异常故障时，按不同故障级别流程，通过电话、短信、邮件等方式通知相关人员进行故障处理。
2. 记录故障发生时间、故障现象、影响范围等信息。按不同的故障问题，判断是否内部处理或者由原设备厂家提供故障处理。
3. 需要对事件的处理全流程进行跟踪，督促相关人员及时处理，确保及时解决。在故障处理完毕对用户进行回访确认。
4. 重大故障解决之后，故障处理人员需针对故障发生原因、解决办法、改进措施、经验总结等方面整理详细故障分析，形成《故障分析报告》。
5. 运维范围内的设备均为备件、人工包干运维，对用户核心设备的故障无法在响应报障的当天现场修复的，应提出应急解决方案，提供备用设备临时替代，保障用户的日常业务不受影响。

4.3.1.1.2服务成果

服务方案，包括人员、实施计划、响应措施、服务质量管理等内容；月度巡检报告；故障处理报告（按需提供）；服务期结束提供项目服务总结报告。

4.3.2软件系统运行维护服务

为加强对软件系统运维工作的统筹，对支撑业务系统运转的支撑环境（为自然资源云专区的数据库、容器、分布式服务框架、OBS、NAS等）进行统一运维。因此，将软件系统运行维护服务分为业务系统运行维护以及业务系统支撑环境运行维护两部分。

4.3.2.1业务系统运行维护服务

包括广东省自然资源一体化数据库（自然资源三维时空数据库）等8个应用共计25个系统（子系统、组件）的运维服务。以下运维服务内容对应的技术服务人员应专岗专用，不得复用于其他运维服务内容。

4.3.2.1.1广东省自然资源一体化数据库（自然资源三维时空数据库）运行维护服务

4.3.2.1.1.1时空数据管理与服务

4.3.2.1.1.1.1服务内容

运维内容包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.1.1.1.1日常维护

针对业务系统，制定日常维护方案，针对系统各方面设定维护项，合理安排维护计划，实施日常维护工作。在软件系统的正常运行过程中，消除系统缺陷、故障异常、软件告警、报错、存在问题等，保障软件系统运行状况良好；消除安全问题，对系统程序安全漏洞及时修复，降低数据缺失风险与负面影响，确保软件系统能够安全运行。

具体维护内容如下：

（1）提供应用系统配置维护

提供业务配置运维服务，针对数据治理、数据管理、数据应用、数据浏览及数据评价等模块提供配置修改服务，具体服务内容包括：

- 1）前端页面菜单模块交互调整，根据用户需求，针对数据治理、数据管理、数据应用、数据浏览及数据评价等模块的前端页面菜单模块的调整，包括模块（工具）顺序调整、删除、名称修改等。
- 2）系统数据更新服务，根据用户需求，聚焦自然资源与国土空间管理核心场景，依托全流程标准化作业体系，针对汇总统计、流量分析、资源本底、规划管控、耕地保护、用途管制、资产权益等各类专题场景页面开展数据更新。
- 3）地图参数调整，根据用户需求，聚焦二三维一体化场景，针对二维地图和三维地图开展地图参数调整，包括初始位置与视角、地图初始层

级、缩放控制、数据加载策略、二三维底图、二三维注记等参数。

4) 数据目录调整, 根据用户需求, 依托最新数据分类规范, 针对数据资源目录、数据应用目录进行调整, 以实现数据资产的精细化管理与高效赋能业务场景。

(2)安全维护服务

对系统、网络、中间件、操作系统等进行安全维护, 按照要求对系统及中间件、操作系统等存在的漏洞进行管理和补丁更新, 优化访问控制与权限管理策略, 提升数据安全与备份技术, 定期开展应急响应, 保障系统持续安全运行。包括但不限于:

1.漏洞管理与补丁更新

定期开展系统、应用、网络设备、中间件、操作系统等安全漏洞的整改, 及时对漏洞进行修复, 安装操作系统、软件、固件的安全补丁, 修复已知漏洞, 修复完成后编制对应的漏洞修复报告。

2.优化访问控制与权限管理策略

对系统、中间件、操作系统等软件、固件进行多因素认证策略, 根据要求进行强密码策略优化, 禁用默认用户, 定期对安全监控和日志等进行分析清理越权、冗余账号。

3.提升数据安全与备份技术

按要求对系统数据加密算法等技术进行升级, 结合业务需要, 制定适宜的备份策略, 定期对全量和增量备份进行可用性测试, 开展恢复流程演练。

4.定期开展应急响应

制定并细化安全事件响应流程, 定期配合开展渗透测试, 对系统安全防护措施进行验证和优化。

(3)性能优化服务。

优化系统代码, 减少冗余计算、优化算法复杂度, 根据系统使用情况提升系统并发能力, 优化缓存机制提升系统性能, 同时保障数据鲜活可用。

根据通过中国信息安全测评中心安全可靠测评的终端性能情况, 优化系统前端和后端性能, 使系统能够在通过中国信息安全测评中心安全可靠测评的终端电脑上流畅显示。

系统性能优化包括但不限于:

1)性能现状诊断

指标采集: 通过性能监控工具获取关键性能数据: 空间查询延迟、数据吞吐量、并发连接数、时空索引命中率、分析任务耗时、内存占用、CPU 利用率、中间件(如MRS)作业延迟。

瓶颈定位: 对比基线数据, 识别性能短板(如空间查询超时、分析任务队列积压、数据加载缓慢)。

2)数据层优化

①时空数据存储与索引

优化时空数据库表结构(如分区存储时间序列数据、分块存储大场景栅格数据)。

重建或新增时空索引、聚合索引, 提升空间查询效率。

清理无效数据(如历史临时缓存、重复轨迹点), 归档低频访问数据至冷存储。

②数据传输与缓存

启用数据压缩, 减少网络传输流量。

引入分布式缓存(如CRedis)或内存存储高频访问的空间数据、元数据、查询结果, 降低数据库压力。

3)服务引擎优化

调整服务线程池参数(如Tomcat最大线程数、负载均衡进程数), 匹配并发访问需求。

优化OGC服务(WMTS/WMS)渲染策略: 开启缓存机制、限制单次查询数据量(如分页加载矢量要素)。

优化时空分析算法, 简化空间叠置分析层级、并行化处理栅格计算任务。

调整分布式计算框架参数(如MRS-Spark分区数), 提升批量数据处理效率。

拆复杂分析任务为微服务, 避免单节点资源耗尽。

4) 性能验证与迭代

压力测试：使用工具（如 JMeter）模拟高并发时空查询、批量分析场景，验证优化后指标（如空间查询响应时间从 5s 降至 2s，分析任务吞吐量提升 50%）。

A/B 测试：对核心功能或服务（如应用分析服务引擎）分版本部署，对比不同优化方案的性能表现。

持续监控：建立常态化性能监控仪表盘，设置阈值告警（如时空索引命中率<70% 触发预警），及时发现新瓶颈。

5) 文档与流程固化

记录优化前后的性能指标对比、配置参数变更，形成《性能优化手册》。

更新系统架构图，标注分布式节点、缓存层、负载均衡设备等关键组件位置。

制定定期性能巡检计划（如每月分析慢查询日志、每季度评估数据增长趋势），提前规划扩容或算法升级。

6) 自动化任务与工具维护

对系统已有的自动化工具、任务计划程序和定时任务进行运维，对任务报错进行及时处理，对性能低下的任务、程序和工具进行优化，提升工具的自动化程度，保障现有任务、工具和程序的稳定正常运行。

4.3.2.1.1.1.1.2例行巡检

定期对系统开展预防性维护服务（巡检），以确保系统的正常运行。通过定期对系统的各项性能指标进行测试，掌握系统使用的增长趋势，及时地升级系统软、硬件，调整系统参数，并为系统支撑平台的升级提供依据。

系统预防性维护主要包括以下内容（不限于）：

1.系统状态检查

应用服务进程运行情况、进程连接数。

数据库运行状态分析、中间件运行状态分析。

网络流量统计、协议分布、出错率统计。

应用的各种接口、工作流、计算模型、任务。

2.用户行为检查

用户系统访问行为。

用户在系统上的增删改行为。

用户对数据库的操作行为。

3.应用系统功能巡检

应用系统功能可用性检查。

应用系统功能稳定性检查。

应用系统功能正确性检查。

应用系统功能完整性检查。

4.3.2.1.1.1.1.3技术支持

（1）系统新对象调试技术支持

1.协助开展系统新工作流、新数据计算模块等对象搭建技术支持工作。在有新的对象需要搭建时，提供新对象搭建、调试服务，配置数据库、工作流定义等，使得新的对象纳入系统管理。

（2）系统改造升级技术支持

1.提供改造服务，针对应用系统的代码功能缺陷，或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求，提供系统迭代服务。需要根据操作系统、数据库、中间件、大数据平台等升级情况，及时对系统进行对应的适配改造，保障系统稳定运行。系统适配升级的内容包括但不限于：

1) 前期评估与准备

①环境调研与依赖分析

梳理各组件对麒麟 V10 操作系统、人大金仓/ DDS 数据库、Credis/华为负载均衡中间件、MRS 大数据平台的依赖关系（如系统内核版本、

库文件、端口协议、API 接口等）。

收集各升级组件的官方文档（如升级说明、兼容性列表、配置变更日志），确认升级后版本的接口变化、配置项调整及性能影响。

②制定适配升级策略

按组件优先级与风险等级排序（如数据库、操作系统为基础组件，优先评估），确定升级顺序（通常遵循“底层基础设施→上层应用”原则，如操作系统→数据库 / 中间件 / 大数据平台→子系统）。

明确适配范围：包括子系统代码、配置文件、数据接口、部署脚本等与升级组件交互的部分。

③搭建测试环境

复制生产环境架构，搭建独立测试环境，包含升级后的麒麟 V10、人大金仓 / DDS、Credis/华为负载均衡中间件、MRS 版本，以及待适配的子系统组件。

准备测试数据集（涵盖典型时空数据类型、业务场景），用于验证适配后的功能与性能。

2）分组件适配升级

①操作系统（麒麟 V10）适配

内核与驱动兼容性：检查子系统依赖的内核模块（如文件系统驱动、网络协议栈）是否支持升级后的内核版本，更新或重新编译不兼容的驱动程序。

库文件与环境变量：确认子系统调用的系统库路径、版本是否变更，调整环境变量或重新链接动态库。

安全策略适配：适配麒麟 V10 的SELinux策略、用户权限管理机制，确保子系统服务启动权限、数据访问控制符合新系统要求。

②数据库（人大金仓、DDS）适配

驱动与连接协议：更新子系统的数据库驱动至兼容新版本（如人大金仓驱动、DDS驱动），验证连接协议（如 TCP/IP 端口、SSL 加密方式）是否变更。

SQL 语法与功能差异：对比新旧数据库版本的 SQL 语法（如存储过程、函数、事务特性），修改子系统中不兼容的查询语句或业务逻辑。

数据迁移与兼容性：若数据库存储引擎或数据格式变更，评估是否需要迁移数据（如人大金仓从旧存储引擎迁移至新引擎），验证数据一致性与完整性。

性能参数调优：根据新数据库版本的优化建议，调整子系统的连接池配置、查询缓存策略等。

③中间件（Credis、华为负载均衡）适配

Credis（缓存中间件）适配：确认子系统使用的 Credis 客户端库是否兼容新版本，调整连接参数（如集群模式配置、密码验证方式）。验证缓存数据结构（如 Key 格式、过期策略）在新版本中的兼容性，处理因协议变更（如 Redis API 差异）导致的逻辑错误。

华为负载均衡（负载均衡服务器）适配：更新华为负载均衡配置文件，适配新版本的指令变化（如负载均衡策略、SSL 证书路径、请求超时时间）。验证子系统的反向代理规则、统一资源定位系统路由是否正常，调整跨域资源共享（CORS）配置以匹配新策略。

④大数据平台（MRS）适配

组件版本兼容性：检查子系统依赖的 MRS 组件（如 Hadoop、Spark、Hive、HDFS、HBase）版本是否兼容，更新 SDK 或 API 调用方式。

数据接口与格式：验证与 MRS 的数据交互接口（如 Spark Streaming 消费数据、Hive 表读写）是否因平台升级导致协议或格式变化，调整数据解析逻辑。

资源调度与性能：根据 MRS 新的资源管理机制（如 YARN 队列配置），优化子系统的任务提交参数、并行度设置，避免资源竞争。

3）集成测试与验证阶段

①功能验证

按业务场景测试子系统功能：

时空数据存储与查询（如通过人大金仓 / DDS 检索空间对象）；

服务接口调用（如通过华为负载均衡暴露的 RESTful API 获取分析结果）；

大数据分析任务（如通过 MRS 执行时空数据分布式计算）。

重点验证跨组件交互逻辑（如子系统通过 Credis 缓存数据库查询结果）是否因升级出现异常。

②性能测试

模拟生产负载，测试子系统在升级环境下的响应时间、吞吐量、资源利用率（如 CPU、内存、IO），对比基线数据，优化瓶颈点（如调整数据库索引、中间件连接数）。

验证大数据作业的执行效率，调整并行任务数、数据分片策略以适配 MRS 新特性。

③兼容性与回归测试

确认子系统在升级后的各组件环境中向下兼容（如支持旧版本数据库备份恢复）。

执行全链路回归测试，覆盖历史缺陷场景，确保升级未引入旧功能故障。

4）部署与切换阶段

①制定部署方案

明确部署步骤（如先升级基础设施组件，再更新子系统服务）、回滚策略（保留旧版本组件安装包、配置备份）。

规划停机窗口，协调相关团队（如运维、业务部门）确保部署期间业务影响最小化。

②分阶段部署

灰度发布：先在部分节点或子网部署升级后的子系统，监控运行状态（如日志异常、接口成功率），逐步扩大范围。

全量切换：确认灰度环境稳定后，完成所有节点的升级，更新负载均衡配置指向新版本服务。

③运行监控与优化

部署后持续监控子系统关键指标（如数据库连接数、中间件请求延迟、MRS 作业成功率），及时处理内存泄漏、线程阻塞等潜在问题。

收集用户反馈，针对实际业务场景进行动态调优（如调整缓存命中率、优化大数据作业调度策略）。

5）文档与知识沉淀

更新《技术手册》，记录各组件升级后的配置参数、适配关键点及已知问题解决方案。

对技术团队进行培训，确保掌握新环境下的系统维护与故障排查方法。

建立版本兼容性清单，为后续升级提供参考（如记录麒麟 V10 与人大金仓某版本的适配经验）。

（3）系统修复或优化

提供系统功能代码优化技术支持，完成系统升级或变更，对系统的缺陷和漏洞进行定期检查，按要求对系统缺陷和漏洞进行修复和优化。

1）系统缺陷修复

系统缺陷是系统在设计、开发、部署或运行过程中产生的非预期错误、功能异常或性能问题，影响系统功能、性能或可用性（如功能崩溃、响应缓慢、数据显示错误等）。系统缺陷本质上属于功能性或非功能性的异常，可能导致用户体验下降或业务流程受阻，影响系统正常使用，但不一定直接涉及安全风险，通常不直接威胁数据安全或系统控制权。系统缺陷修复的包括但不限于：

①缺陷定位与确认

通过用户反馈、系统日志、监控工具（如时空数据访问异常日志、服务响应超时记录）识别缺陷现象。

复现缺陷，验证其在时空数据存储、管理、查询、分析或可视化等环节的触发条件与稳定性。

②缺陷分析与评估

分析缺陷根源（如时空数据格式解析错误、坐标系转换异常、空间索引失效、服务接口参数错误等）。

评估影响范围（如特定区域数据查询失败、时间序列数据丢失、可视化渲染错位）及优先级（是否影响核心业务流程或安全合规）。

③修复方案设计

针对时空数据特性制定方案（如修正空间数据拓扑错误、优化时空索引策略、调整时间同步机制、完善坐标转换算法等）。

确保方案兼容现有时空数据标准（如 OGC 规范）与系统架构，避免破坏时空数据一致性。

④开发修复与测试

开发人员修改代码或配置（如更新空间数据处理模块、修复时间戳解析逻辑），同步更新数据字典与接口文档。

进行时空数据专项测试：

单元测试：验证单个功能模块（如坐标转换函数）的正确性。

集成测试：验证多模块协同（如数据存储与查询服务）的时空一致性。

回归测试：确保修复未影响历史时空数据查询、时空分析结果准确性。

⑤部署与验证

在预生产环境进行灰度部署，验证系统功能的可用性、稳定性、预期效果、响应速度、数据精度（如空间几何图形完整性、时间戳准确性）。

正式部署至生产环境，同步更新版本号，记录变更涉及的数据范围与服务接口。

⑥闭环管理与优化

监控生产环境时空数据访问日志、服务性能指标（如空间查询延迟、时间序列吞吐量），确认缺陷已解决。

归档修复记录（含缺陷类型、修复方案、测试结果），补充至知识库。

分析缺陷诱因，优化系统功能缺陷修复质量控制流程（如增加数据入库前的时空校验规则）或服务监控策略（如实时预警空间索引失效）。

2）系统漏洞修复

系统安全漏洞是系统中存在的可被攻击者利用，从而导致数据泄露、系统控制或服务中断等安全事件的弱点，直接威胁系统安全（如数据泄露、权限滥用、恶意代码执行等）。系统安全漏洞本质上直接关联安全风险，是攻击者可能利用的“入口”，具有被恶意利用的潜在性，可能被攻击者利用引发安全事件，造成隐私泄露、资产损失或法律风险。系统安全漏洞修复包括但不限于：

①漏洞识别与验证

通过安全扫描工具、渗透测试或漏洞库匹配，发现安全弱点（如未经授权访问、垂直越权访问、时空数据查询接口 SQL 注入、相关组件安全漏洞等）。

验证漏洞真实性与可利用性，确认影响范围（如涉及的功能模块、服务接口、用户权限层级）。

②风险评估与优先级排序

评估漏洞的安全风险等级（如高危、中危、低危），结合业务影响（如是否导致时空数据泄露、服务中断或被恶意篡改）确定修复优先级。

重点关注涉及时空数据隐私或关键基础设施的漏洞。

③修复方案制定

针对漏洞类型制定技术方案：

认证授权漏洞：增强身份验证机制（如多因素认证）、细化时空数据访问权限（如按区域 / 时间粒度控制）。

注入类漏洞：采用参数化查询、输入校验（如限制空间坐标格式、时间戳范围）、避免 SQL / 代码注入。

组件漏洞：升级相关组件至安全版本，或替换存在漏洞的库文件。

数据传输漏洞：启用 HTTPS 加密传输时空数据，配置 TLS 协议最小版本限制。

制定临时防护措施（如封禁异常 IP 访问、关闭非必要时空服务接口），降低修复前的攻击风险。

④开发修复与安全测试

开发人员实施代码修复或配置加固，同步更新安全设计文档（如访问控制策略、加密方案）。

⑤进行安全验证测试：

漏洞验证测试：使用攻击工具验证漏洞是否已消除。

渗透测试：模拟攻击者尝试利用时空数据接口或存储层漏洞，验证修复有效性。

合规性测试：确保修复符合数据安全法、个人信息保护法及行业标准（如地理信息安全要求）。

⑥部署与监控

在预生产环境进行漏洞修复验证，监控时空数据服务的安全性指标（如异常访问日志、加密传输效率）。

部署至生产环境后，实时监控漏洞相关攻击行为（如针对已修复接口的异常请求），启用入侵检测系统（IDS）或安全信息和事件管理（SIEM）工具。

⑦闭环管理与复盘

确认漏洞修复后，更新漏洞管理台账，记录修复时间、版本号及涉及的系统资产。

复盘漏洞产生原因（如开发阶段未进行安全编码、组件更新不及时），优化安全开发生命周期流程，增加时空数据安全编码规范与组件安全扫描环节。

对相关人员进行安全培训（如时空数据隐私保护、安全编码实践），提升团队安全意识。

4.针对系统中各类查询统计报表功能的完善、调整、配置及维护。主要对存在特殊要求的且系统已有查询或汇总分析功能不满足统计分析需求的，提供技术分析、数据辅助查询、安全事件建模、数据关联输出等技术支持服务。

5.在两会、国庆或网络安全重点保障期间，保障系统的正常运行，为安全调查分析人员开展网络安全保障监控提供应急支持服务，保障系统的正常运行。

6.按要求部署安全防护软件，部署防火墙、杀毒软件等，拦截恶意攻击。

4.3.2.1.1.1.4故障处理

要求对系统故障进行处理。根据系统故障大小等级建立响应机制，对业务不产生影响或影响较小的故障，视情况而定是否需要现场处理；对业务产生较大或重大影响的故障，需4小时内到达现场，期间保持远程技术支持。到达现场后，4小时内系统恢复运行。包括但不限于：

(1)网络故障。查看服务器或客户端系统网络状态，查看服务端口是否正常开启。如无法解决联系网络维护人员或网络供应商解决。

(2)服务器故障。服务器端软件无法使用,查看任务管理器和事件日志,记录出错的信息并判断。关闭相应的服务器进程,并重新启动该服务器进程，查看数据库连接是否正确，查看数据库服务器是否运行正常。如判定为服务器程序崩溃，请求重装程序。

(3)操作系统故障。经判断为服务器操作系统层面的故障后,在采取任何措施之前,应该备份故障服务器上所有相关数据,并确定通过备份数据可以至少把服务器恢复到故障发生时的初始状态(即保护现场)，在确定任何一步操作有回复的途径之前,不应该进行该操作。查看任务管理器,记录资源使用状况以及各个进程详细情况，以备后续判断。

(4)系统故障。操作前备份所有系统数据和业务数据，查看系统日志，根据日志情况，制定相应的解决方案，实施故障修复。制定好系统版本管理，故障不可修复时进行版本回滚，或重建系统。

4.3.2.1.1.1.2服务成果

系统月度巡检报告，内容需包括例行巡检内容；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.1.2时空图谱管理与服务

4.3.2.1.1.2.1服务内容

运维内容包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.1.2.1.1日常维护

针对业务系统，制定日常维护方案，针对系统各方面设定维护项，合理安排维护计划，实施日常维护工作。在软件系统的正常运行过程中，消除系统缺陷、故障异常、软件告警、报错、存在问题等，保障软件系统运行状况良好；消除安全问题，对系统程序安全漏洞及时修复，降低数据缺失风险与负面影响，确保软件系统能够安全运行。

具体维护内容如下：

(1)日志检查服务

通过日志管理系统或其他查询手段检查系统运行情况，及时发现系统运行过程中的问题，包括但不限于执行路径异常、参数和性能异常等，为系统正常运行提供保障。

(2)应用系统维护

1.监控日常运行状态，跟踪系统功能模块及时处理异常情况；管理各模块，维护各模块的接口、工作流、计算模型、任务和数据。按要求对工作流、计算模型、任务和数据进行增加、变更、删除、备份。

2.系统缺陷修复优化，对系统的缺陷和漏洞进行定期检查，按要求对系统缺陷进行修复和优化。

3.系统性能优化，在系统使用过程中由系统缺陷、网络、资源瓶颈等情况产生的性能问题，定期开展性能测试评估，制定性能优化方案，实施性能优化工作。

4.系统适配升级，根据操作系统、数据库、中间件、大数据平台等升级情况，及时对系统进行对应的适配改造，保障系统稳定运行。

4.3.2.1.1.2.1.2例行巡检

定期对系统开展预防性维护服务（巡检），以确保系统的正常运行。通过定期对系统的各项性能指标进行测试，掌握系统使用的增长趋势，

及时地升级系统软、硬件，调整系统参数，并为系统支撑平台的升级提供依据。

系统预防性维护主要包括以下内容（不限于）：

1.系统状态检查

应用服务进程运行情况、进程连接数。

数据库运行状态分析、中间件运行状态分析。

网络流量统计、协议分布、出错率统计。

应用的各种接口、工作流、计算模型、任务。

2.用户行为检查

用户系统访问行为。

用户在系统上的增删改行为。

用户对数据库的操作行为。

4.3.2.1.1.2.1.3技术支持

1.协助开展系统组件测试和部署、新工作流、模块接入等工作。在有新的应用系统需要接入系统时，提供新对象接入调试服务，配置数据库、工作流定义等，使得新的对象纳入系统管理。

2.对广东省自然资源一体化数据库（自然资源三维时空数据库）提供改造服务，针对应用系统的代码功能缺陷，或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求，提供系统迭代服务。

3.系统功能代码优化，协助完成系统升级或变更。

4.针对系统中各类查询统计报表功能的完善、调整、配置及维护。主要对存在特殊要求的且系统已有查询或汇总分析功能不满足统计分析需求的，提供技术分析、数据辅助查询、安全事件建模、数据关联输出等技术支持服务。

5.在两会、国庆或网络安全重点保障期间，保障系统的正常运行，为安全调查分析人员开展网络安全保障监控提供应急支持服务，保障系统的正常运行。

4.3.2.1.1.2.1.4故障处理

要求对系统故障进行处理。根据系统故障大小等级建立响应机制，对业务不产生影响或影响较小的故障，视情况而定是否需要现场处理；对业务产生较大或重大影响的故障，需4小时内到达现场，期间保持远程技术支持。到达现场后，4小时内系统恢复运行。包括但不限于：

(1)网络故障。查看服务器或客户端系统网络状态，查看服务端口是否正常开启。如无法解决联系网络维护人员或网络供应商解决。

(2)服务器故障。服务器端软件无法使用,查看任务管理器和事件日志,记录出错的信息并判断。关闭相应的服务器进程,并重新启动该服务器进程，查看数据库连接是否正确，查看数据库服务器是否运行正常。如判定为服务器程序崩溃，请求重装程序。

(3)操作系统故障。经判断为服务器操作系统层面的故障后,在采取任何措施之前,应该备份故障服务器上所有相关数据,并确定通过备份数据可以至少把服务器恢复到故障发生时的初始状态(即保护现场)，在确定任何一步操作有回复的途径之前,不应该进行该操作。查看任务管理器,记录资源使用状况以及各个进程详细情况，以备后续判断。

(4)系统故障。操作前备份所有系统数据和业务数据，查看系统日志，根据日志情况，制定相应的解决方案，实施故障修复。制定好系统版本管理，故障不可修复时进行版本回滚，或重建系统。

4.3.2.1.1.2.2服务成果

系统月度巡检报告，内容需包括例行巡检内容；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.1.3影像智能识别管理与服务子系统（含遥感影像智能识别基础框架）

4.3.2.1.1.3.1服务内容

运维内容包括对影像智能识别管理与服务（含遥感影像智能识别基础框架）开展日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.1.3.1.1日常维护

在系统运行维护方面，制定日常维护方案，针对系统的多框架兼容、依赖库、算法库、用户角色权限、样本数据管理、模型文件迭代、解译

生产服务管理、中间件、系统运行基础设施等方面的维护项，合理安排维护计划。在系统安全维护方面，消除故障异常、解决存在问题、排查安全隐患等，保障系统运行状况良好。影像智能识别管理与服务子系统日常维护内容包括但不限于：

（1）日志检查服务通过日志管理系统其它查询手段检查系统运行情况，及时发现系统运行过程中的问题，包括但不限于执行路径异常、参数和性能异常等，为系统正常运行提供保障。

（2）样本及模型维护：日常监督样本质量、辅助样本上传导入；开展模型性能优化，提高模型精度

（3）性能调优：定期开展系统性能测试，例如数据传输测试、样本查询测试、模型训练测试等，根据系统反应情况，提出优化建议，包括数据库调优、代码优化、架构调整等，提升系统性能和响应速度。

（4）多框架兼容维护：维护不同深度学习框架的版本兼容性，解决框架的依赖冲突。

（5）依赖库更新维护：及时更新系统依赖库，并同步解决兼容问题。

（6）算法维护：对基础框架内置算法、API等进行维护和测试。

（7）缺陷优化：系统在运行过程中存在的功能缺陷，及时进行修复优化。

（8）配置管理：采用配置自动化、版本回滚等方式，对基础设施和应用的配置项进行记录、跟踪、变更和管理。

（9）备份与恢复：优化备份策略，验证备份文件的可恢复性。

4.3.2.1.1.3.1.2例行巡检

(1)系统资源巡检

检查服务器CPU、内存、磁盘使用率、负载状态，对于异常状态的系统资源及时处理，保持资源的可用性。

(2)应用系统巡检工作

包括对平台系统各个模块功能的检查，保证功能和模块运行正常；应用系统冗余及缓存检查，保证系统运行速率。

(3)有效账户巡检

检查用户数量及用户角色配置、所属部门、权限是否正确，维护账户权限，清除测试账号、僵尸账号。

(4)巡检记录

根据巡检情况，每月完成巡检记录报告。

4.3.2.1.1.3.1.3技术支持

（1）系统维护与升级：针对应用系统的代码功能缺陷，或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求，提供系统迭代服务，或根据新的业务需求协助完成系统功能升级改造或变更。

（2）样本及模型更新：协助开展子系统中样本库数据整理更新入库、迭代更新后模型效果测试以及应用模型服务发布等。

（3）信息更新：开展系统中算法库更新、API维护、扩充示例脚本等。

（4）用户体验优化：在系统运行过程中，通过问卷、访谈等方式搜集用户使用反馈信息，整理并进行问题跟踪，协调开发团队针对性开展系统优化。

（5）安全加固：配合相关部门对系统进行安全扫描，对安全整改意见及时响应处理。

（6）特殊时期维护：在两会、国庆或网络安全重点保障期间，保障系统的正常运行，为安全调查分析人员开展网络安全保障监控提供应急支持服务，保障系统的正常运行。

（7）培训与文档：进行运维人员相关技术培训，以及对用户进行培训，使其深入了解系统。提供操作手册、运维手册等辅助文档。建立系统知识库，整理常见问题及解决方案。

4.3.2.1.1.3.1.4故障处理

要求对系统故障进行处理。根据系统故障大小等级建立响应机制，对业务不产生影响或影响较小的故障，视情况而定是否需要现场处理；对业务产生较大或重大影响的故障，30分钟内响应，需4小时内到达现场，期间保持远程技术支持。到达现场后，4小时内系统恢复运行。故障处理包括但不限于：

（1）网络故障。查看服务器或客户端系统网络状态，查看服务端口是否正常开启。如无法解决联系网络维护人员或网络供应商解决。

（2）服务器故障。服务器端软件无法使用，查看任务管理器 and 事件日志,记录出错的信息并判断。关闭相应的服务器进程，并重新启动该服务器进程，查看数据库连接是否正确，查看数据库服务器是否运行正常，如判定为服务器程序崩溃，请求重装程序。

(3)操作系统故障。经判断为服务器操作系统层面的故障后，在采取任何措施之前，应该备份故障服务器上所有相关数据，并确定通过备份数据可以至少把服务器恢复到故障发生时的初始状态(即保护现场)，在确定任何一步操作有回复的途径之前，不应该进行该操作，查看任务管理器，记录资源使用状况以及各个进程详细情况，以备后续判断。

(4)系统故障。操作前备份所有系统数据和业务数据，查看系统日志，根据日志情况，开展系统故障修复。做好系统版本管理，故障不可修复时进行版本回滚。

4.3.2.1.1.3.2服务成果

影像智能识别管理与服务子系统巡检月报；

影像智能识别管理与服务子系统故障处理报告（按需提供）；

影像智能识别管理与服务子系统运维服务总结报告。

4.3.2.1.2广东省自然资源一体化管理与服务平台（国土空间基础信息平台）运行维护服务

4.3.2.1.2.1广东省自然资源决策参阅子系统

对广东省自然资源决策参阅子系统提供日常维护、例行巡检、技术支持以及故障处理服务。

4.3.2.1.2.1.1日常维护

对系统提供日常维护服务，主要包括资源管理、权限管理、版本发布管理、功能配置等，建立服务器、存储等资源的全生命周期动态台账，实现负载监控与扩缩容支持的闭环；基于实施账号权限最小化原则，对系统账号权限进行全流程管理，同时，开展账号日志审计与异常权限调整处理工作；遵循非高峰发布、预测试验证、灰度升级（单节点/集群滚动）灰度升级（单节点/集群滚动）等，确保版本迭代工作规范进行；同时提供系统功能配置优化服务，提升系统的业务适配性；形成“资源可溯、权限可控、发布可靠、配置高效”的日常维护模式，确保快速响应，保障系统稳定运行。日常维护主要工作内容如下：

4.3.2.1.2.1.1.1资源管理

梳理决策参阅系统的各类业务信息，记录业务资源的状态、进度、关联关系等关键信息。定期检查业务资源的使用情况，及时发现并处理资源冲突和异常。根据业务需求，对业务资源进行合理分配和调度，提高协同工作的效率。

4.3.2.1.2.1.1.2权限管理

提供权限管理服务，遵循最小权限原则与安全审计要求，集中管理运维相关账号，管控运维人员访问权限，仅允许授权人员通过可信网络接入；定期复核权限分配策略，调整权限、处理闲置账号，确保与安全管理要求一致；记录留存运维过程中的会话日志，支持事后追溯与合规审查。每月审查账号权限，确保符合最小权限原则和安全政策；审查操作系统关键角色权限、数据库权限、中间件权限、非结构化存储权限等，定期更新账号密码，保障系统及数据安全。系统变更或业务需求变化时，及时调整基础软件角色权限，保证时效性和准确性，支撑运维工作。低权限用户联调或排错需提权时，进行临时赋权，操作完成后及时回收权限，遵循最小权限原则。根据用户状态更新或回收账号，如账号所有者离场时回收其权限。

对应用账号建立覆盖全生命周期管理体系，包括账号的规范化创建、权限动态调整、离职/转岗账号冻结或注销等流程。按角色、业务场景精细化授权，确保权限最小化原则，避免越权访问。需定期开展账号权限审计，核查冗余账号、异常权限分配（如超管权限滥用），针对临时账号（如等保测评、密评等）需建立审批流程与时限控制机制，防范权限泄漏风险。

4.3.2.1.2.1.1.3系统版本发布

提供系统版本发布服务，对资源资产、规划配置、管制利用、保护修复模式的版本需要更新时，需对系统发布进行规划，且需完成相关测试，验证新版本系统功能正常运行后，才能进行正式的发布。若验证不通过，需要将新版本回退到原有版本。主要流程如下：

1、发布版本规划：确定发布计划，包括日期、内容、范围、方式、流程步骤、任务、责任人及时间节点等；确定发布时间，综合考量业务需求等因素，选在业务低峰期；制定备份策略，对系统文件、配置文件、数据库进行全量备份。

2、发布版本申请：按变更管理规范流程申请变更，审核人审核版本变更目标、时间计划、影响范围、风险评估及应对措施。

3、执行版本发布：单节点升级时，停止服务、执行升级、更新配置文件、启动服务并验证状态；集群滚动升级分批进行，通过负载均衡器路由流量；分布式系统升级分阶段进行，避免服务中断；功能验证时测试验证系统核心功能，检查日志及监控指标。发布测试验证不通过时，停止新版本服务，从备份恢复旧版本及配置文件，记录回滚原因及操作步骤，生成回滚报告。

4、系统更新后全链路验证：针对版本升级或配置调整，模拟真实用户操作路径，覆盖核心业务流程，验证功能完整性与业务连续性；开展高

并发、异常场景压力测试，确保系统稳定性与容错能力。

5、持续监控与效果闭环：优化后通过AB测试、用户回访验证效果，确保版本发布后问题解决率达标。建立用户体验指标体系（操作成功率、响应时间），长效跟踪系统使用情况。

4.3.2.1.2.1.1.4日常功能配置

提供日常功能配置服务，主要包括对多端界面展示规则定制、业务指标动态管理、智能预警阈值设定以及数据汇聚接口调整等工作，支撑桌面端、移动端以及汇报端的三端协同智能化决策场景。针对高频配置场景，需提供模板化配置工具，提升效率并降低人工操作风险。所有配置操作需留存完整日志，支持事后追溯审计。

4.3.2.1.2.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

4.3.2.1.2.1.2.1业务监控

提供业务功能监控服务，针对小绿书、亮灯系统、综合态势核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

4.3.2.1.2.1.2.2业务功能巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，页面响应时间>1000ms告警。

4.3.2.1.2.1.3技术支持

对系统提供技术支持服务，主要包括以下内容：通过标准化变更流程（需求评估、灰度发布、回滚验证）与配置管理数据库动态维护，保障系统变更可追溯、风险可控；围绕安全漏洞修复（版本升级、基线加固、弱密码整改）等保测评合规改造，提升系统抗风险能力；针对性能瓶颈开展架构调优（容器资源弹性扩缩、微服务链路治理），结合全链路压测验证效能提升；建立应急重保专班，按预案执行故障隔离、资源调配及快速恢复，完善“演练—处置—复盘”闭环；同步支撑功能配置动态调整、数据完整性维护及用户问题实时响应，形成“事前预防—事中控制—事后优化”的一体化响应体系，确保系统稳定性、安全性与业务连续性高效协同。具体服务内容如下：

4.3.2.1.2.1.3.1变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、数据增删改、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求申请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

（2）变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。

（3）变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。

（4）变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

4.3.2.1.2.1.3.2配置管理

提供配置管理服务，规范整个系统的配置管理流程。建立和维护标准化、系统化的配置管理台账，确保所有配置项都得到记录和控制。配置

管理的服务内容如下：

- （1）配置关系梳理：确认配置范围、定义和标识配置项，梳理关联关系，制定配置管理机制、变更与审核流程机制、文档管理机制，形成体系化配置管理数据库。
- （2）配置数据录入：明确配置管理数据库所需配置信息和清单，录入配置项信息，确保准确性、适用性和可维护性。
- （3）配置数据更新：根据系统版本发布和变更情况，发起配置任务，更新配置库环境和调整配置基线；建立定期审查计划，排查与实际情况不匹配的情况；定期备份配置库，防止数据丢失。

4.3.2.1.2.1.3.3系统安全管理

提供系统安全管理服务，规范系统安全风险从问题接收、整改到验证的整个流程，具体服务内容如下：

- （1）安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。
- （2）安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。
- （3）安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。
- （4）整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。
- （5）整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改问题报告。

4.3.2.1.2.1.3.4应急与重保统筹组织

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

- （1）应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。
- （2）应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。
- （3）应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。
- （4）应急与重保支持：定期组织应急与重保支持，模拟不同应急场景，验证预案可行性和团队协作效率，记录薄弱环节以便优化。
- （5）应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

4.3.2.1.2.1.3.5系统优化

对决策参阅系统的性能进行优化，通过优化成果展示算法等方式，提高系统的数据处理效率和存储容量。对系统的架构进行评估和优化，提高系统的可扩展性和稳定性。针对基础软件运行架构的缺陷，或由于故障、安全等要求提出的需求，对系统运行架构环境进行调优与完善，提升应用的响应速度。对系统在高并发、大数据量场景下的性能瓶颈，提出应用优化方案，包括但不限于缓存策略调整、异步任务拆分、连接池调整等。优化后进行压力测试和性能基准测试，提供基准测试结果对比，量化性能提升效果。

4.3.2.1.2.1.3.6安全加固

提供应用系统安全加固，侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固；如越权访问、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶

段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

4.3.2.1.2.1.3.7备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日志分析及及时提供技术支持，确保备份策略正常运行。

4.3.2.1.2.1.3.8业务支持

面向系统用户提供业务支持，围绕自然资源资产、规划配置、管制利用、保护修复等四大业务领域提升用户在使用系统时的业务体验，在遇到疑问时能够及时获得相应的指引与建议。

4.3.2.1.2.1.4故障处理

对系统开展故障处理服务，以快速响应、精准定位、闭环管理为核心，构建覆盖“接收—分级—处置—验证—复盘”的规范化故障处理机制：通过监控告警、用户上报等多渠道接收故障，按业务影响分级响应，分派至对应团队紧急处置（如操作系统内核修复、数据库一致性恢复、中间件配置调优、网络拓扑排查及应用层服务重启等），结合日志分析、链路追踪定位根因，实施代码修复、环境回滚或资源扩容等方案；处置后通过全链路验证（功能、性能、数据一致性）确认恢复，释放临时资源并标准化配置；同步启动问题管理，对未根治故障及潜在缺陷进行根因分析，形成《问题报告》并沉淀至知识库，优化应急预案与监控策略；针对应用BUG，严格遵循“环境复现—测试验证—灰度发布”流程，确保修复代码安全上线，最终通过跨团队协作与经验复用，实现故障响应时效、修复质量及系统健壮性的三重提升，降低同类问题复发风险。故障处理工作主要包括以下具体工作内容：

4.3.2.1.2.1.4.1故障管理

整合故障反馈渠道，安排专人通过监控告警、巡检识别或用户上报等渠道发现接收故障需求，记录故障情况。一是初步识别故障，判断类型和影响范围，按业务重要性和影响范围划分故障等级和处置优先级。二是根据故障级别和类型，分派任务至对应运维人员处理，依据机制向相关人员通报故障情况和进度，记录时间节点。三是深入分析故障，制定处置方案，经领导同意后按职责实施处置。四是故障处理结束后，验证处理结果，检查系统运行情况和关键指标是否恢复正常，若未根本解决则记录信息和意见，触发问题解决与管理及变更管理流程。五是若处理过程中涉及临时增加资源的，需在完成故障处理闭环后，删除临时文件，释放系统资源，恢复配置或策略至标准状态，避免二次故障。故障修复一周内，总结故障经验形成报告，对重大故障启动复盘会议，优化应急预案和监控策略。

4.3.2.1.2.1.4.2问题管理

收集问题途径包括未根本解决的故障、日常巡检与监控告警、日志分析等，详细记录问题情况。判断问题类型与影响范围，组织技术专家联合进行根因分析，明确是否为已知错误或新发缺陷，提出处置与改进建议。根据建议制定处理计划，验证可行性后严格执行，防止故障再次发生和引入二次风险。问题发起方验证处理结果，确认解决且无副作用，比对运维基线数据，记录验证结果于《问题报告》。复盘分析问题根本原因，探讨从运维管理、系统架构设计、技术选型等方面优化，避免类似问题再次发生，沉淀为运维知识库案例。关闭前核对处理记录、验证结果及相关文档完整性，经双方签字确认；涉及配置修改或软件升级时，需变更管理流程审批，实施后回归测试确保未复发。

4.3.2.1.2.1.4.3应用缺陷修复

依据缺陷描述搭建与生产环境高度一致的测试环境，依照操作步骤执行复现，详细记录操作及系统响应，形成复现报告。运用工具和日志分析，结合复现报告定位代码错误位置和逻辑错误，深入剖析原因及对其他模块的影响。按修复方案进行代码修改，开展单元测试、集成测试、系统测试，验证修复后代码的正确性、集成情况及系统稳定性可靠性。制定发布计划，对修复代码打包部署前检查，按计划在生产环境发布，发布过程中监控系统运行状态，发布后验证并收集用户反馈。

4.3.2.1.2.1.4.4常见故障处理

在系统发生故障时（如服务不可用、页面卡顿、服务调用异常等）需及时响应，优先通过应用层配置调整恢复业务；通过日志分析、链路追

踪等手段定位根因，并要输出故障分析报告，故障排除后需要进行复盘，并提出相应的改进措施纳入应急预案；建立常见故障知识库，降低同类问题复发概率。

4.3.2.1.2.1.5服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.2.2赋能中心(技术核查工具)

4.3.2.1.2.2.1服务内容

运维内容包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.2.2.1.1日常维护

提供日常维护服务。制定应用功能日常维护方案，针对系统进程、系统接口、系统权限、系统资源、业务保障等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，周期性开展常规维护保养工作，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够7×24小时正常运行。维护对象为应用程序。同时按照标准规范对软件系统进行管理，定期形成系统运行简报。具体维护内容如下：

1.业务维护：利用管理员账号登录系统查看系统操作日志，监控是否有非法的数据删除、异常登入、登出操作等信息。定期查看系统日志，操作日志，判断是否有运行错误信息，定期备份日志等操作。

2.访问管理：系统的用户管理服务，包括：用户账户、权限、组织架构的新增、变更、删除。依据流程分配软件系统的账号和权限，权限以最小原则分配，并对登录日志和权限进行定期审查。根据接入管理的标准规范，设置密码复杂度和登录次数限制等规则。

3.软件版本升级：进行软件版本的维护服务前，制定维护方案和回退方案，方案通过审核后，通过服务提供商的技术支持进行维护操作，进行简单流程的变更，并协助用户下载系统应用的补丁程序及软件升级程序，及时协助或提供安装升级服务，不涉及开发和调测等。完成软件版本的维护服务后应出具相应的版本说明。

4.日志管理：对软件系统的日志采集、展现和检查分析。日志展现围绕资源的整个生命周期，体现资源的具体操作、操作时间、操作人、操作结果等信息。通过对系统日志进行巡查、抽查和定向检查，提早发现执行路径异常、参数和性能异常。

5.报表统计：统计各类资源的用户使用量、每类资源的使用情况，如业务系统的CPU、内存、存储、IP的资源总量及占用量。按照天、周、月、季度的频率周期性生成报表。

6.配置管理：使软件系统各种配置信息得到有效、完整、可追溯的记录归档和维护。配置信息包括：软件系统及其运行环境中所有相关的IT设备、系统及其配置信息；各IT设备、系统之间的物理和逻辑关系。

7.安全加固：根据测评有关要求，完成应用功能的漏洞修复服务，确保通过相关测评，提升系统运行的安全性。

8.操作系统维护：更新操作系统的系统补丁，清理冗余日志，不定期测试系统性能等。

4.3.2.1.2.2.1.2例行巡检

提供定期巡检服务。制定例行巡检方案，针对性能容量、可用性、可连续性、可管理性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现软件系统的故障异常、软件告警、潜在问题、安全隐患等，并及时作出适当的处置，保障软件系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够7×24小时正常运行。

对应用程序等方面进行例行巡检。同时利用已有监控系统，按照标准规范要求进行监控操作，密切注意软件系统情况。检查过程中同步记录运行数据，如若发现任何异常情况应及时进行登记，及时通知相关人员进行处理并跟进处理情况，每月形成巡检报告。

例行巡检主要包括以下内容：

1.日常检查

1) 应用服务运行情况；

2) 日志是否有报错信息；

3) 备份配置文件；

- 4) 备份重要运行日志;
- 5) 清除过期日志;
- 6) 交易连接正常性测试;
- 7) 系统数据库运行状态;
- 8) 系统主要进程运行状态。

2.性能检查

- 1) 业务CPU使用峰值情况;
- 2) 业务内存使用峰值情况;
- 3) 业务会话连接数情况

3.脆弱性检查

- 1) 重要运行程序是否有保留备份;
- 2) 系统配置是否符合运行的要求;
- 3) 系统使用资源是否超过预定阈值。

4.系统业务检查

- 1) 通过进程及日志, 查看应用后台进程, 查看程序进程是否存在;
- 2) 通过页面拨测, 检查功能模块。

5.系统应用服务器检查

- 1) 查看当前磁盘空间/文件系统使用率、空闲空间情况, 查看各挂载点使用及剩余空间;
- 2) 查看当前CPU使用率, 内存使用情况, 查看当前系统资源消耗情况;
- 3) 查看系统监听的端口, 端口能否通畅。

6.系统数据库服务器检查

- 1) 查看服务器磁盘空间, 检查磁盘剩余空间;
- 2) 查看备份作业, 检查作业操作历史记录是否正常;
- 3) 查看表空间占用率, 磁盘空间>90%发告警;
- 4) 查看临时表空间占用率, 磁盘空间>90%发告警。

4.3.2.1.2.2.1.3技术支持

提供7×24小时技术服务, 包括应用功能的技术支持服务; 通过现场服务、远程服务以及热线电话等方式, 对技术核查工具的日常咨询、故障问题、安全加固专项任务、数据统计、服务投诉等服务请求进行登记, 根据事件的性质、类别、等级进行判断, 分派相关人员进行处理, 并对事件处理全流程进行跟踪监督, 确保服务请求得到及时的响应与处理。技术支持服务内容包括:

- 1.远程服务: 在运维服务期阶段, 针对出现的系统故障, 技术人员将远程进行故障的快速修复, 保障系统正常运行。
- 2.现场服务: 在运维服务期阶段, 现场服务包括专业保障人员的现场服务、系统故障出现时的现场服务(用户认为有必要到现场)、重大节假日及重要事件或特殊演示现场服务、特殊、重大报道期间的现场服务。针对不同的现场服务内容派出不同专业的经验丰富的技术人员, 服务内容包括但不限于现场咨询、故障维修、产品或系统升级、特殊演示等。
- 3.服务电话: 在运维服务期阶段, 安排技术支持工程师提供技术支持, 提供7×24小时服务电话。
- 4.电子邮件: 可以通过电子邮件将技术支持请求发送到运维服务组, 技术人员在接到报告之后, 会立即与项目单位取得联系, 为其提供相应的技术支持服务。服务团队也将通过电子邮件为项目单位提供解决方案, 或者根据业务系统需要发送相关的技术资料。

4.3.2.1.2.2.1.4故障处理

提供故障处理服务。当发生故障时, 按照故障定级和处理流程, 及时响应, 快速抢通故障点, 尽早恢复业务, 将故障对业务所造成的负面影响降到最低。在处理完毕后清理现场, 提供故障处理简报。具体故障处理如下:

- 1.应用软件出现无法启动软件可执行文件时, 提前准备好各类需维护软件安装程序, 将应用软件数据文件备份后, 重新安装。
- 2.应用软件打开过程中或运行中异常错误关闭, 准备好安装程序, 操作系统优化和修补软件, 查杀病毒软件, 判断出错原因, 备份数据, 采

取相关修复措施。

3.操作系统出现系统异常或系统资源占用严重，应准备好系统检查程序及修补程序，以及查杀病毒软件，告知使用者错误原因可能类型，提出解决方案，经使用者认可后采取相应措施。

4.操作系统为B/S结构系统，浏览器异常或无法下载控件，准备修复浏览器软件、查杀病毒软件，检查浏览器选项设置，分析原因进行修复。

5.账号密码登录错误，检查账号密码是否有错误或重新分配。

6.系统未响应或无法访问，关闭系统，重新访问；检查系统访问地址是否有误，网络是否正常，端口是否正常，服务器是否正常开启。

7.系统反应缓慢，检测机器性能是否因过低而引起。

8.系统端口不通，检测端口是否被占用，更换端口。

4.3.2.1.2.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.2.3赋能中心(资讯库)

4.3.2.1.2.3.1服务内容

运维内容包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.2.3.1.1日常维护

提供日常维护服务。制定应用功能日常维护方案，针对系统进程、系统接口、系统权限、系统资源、业务保障等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，周期性开展常规维护保养工作，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够7×24小时正常运行。维护对象包括但不限于应用程序、数据库、操作系统等。同时按照标准规范对软件系统进行管理，定期形成系统运行简报。具体维护内容如下：

1.业务维护：利用管理员账号登录系统查看系统操作日志，监控是否有非法的数据删除、异常登入、登出操作等信息。定期查看系统日志，操作日志，判断是否有运行错误信息，定期备份日志等操作。

2.访问管理：系统的用户管理服务，包括：用户账户、权限、组织架构的新增、变更、删除。依据流程分配软件系统的账号和权限，权限以最小原则分配，并对登录日志和权限进行定期审查。根据接入管理的标准规范，设置密码复杂度和登录次数限制等规则。

3.软件版本升级：进行软件版本的维护服务前，制定维护方案和回退方案，方案通过审核后，通过服务提供商的技术支持进行维护操作，进行简单流程的变更，并协助用户下载系统应用的补丁程序及软件升级程序，及时协助或提供安装升级服务，不涉及开发和调测等。完成软件版本的维护服务后应出具相应的版本说明。

4.日志管理：对软件系统的日志采集、展现和检查分析。日志展现围绕资源的整个生命周期，体现资源的具体操作、操作时间、操作人、操作结果等信息。通过对系统日志进行巡查、抽查和定向检查，提早发现执行路径异常、参数和性能异常。

5.配置管理：使软件系统各种配置信息得到有效、完整、可追溯的记录归档和维护。配置信息包括：软件系统及其运行环境中相关的IT设备、系统及其配置信息；各IT设备、系统之间的物理和逻辑关系。

6.安全加固：根据测评有关要求，完成应用功能的漏洞修复服务，确保通过相关测评，提升系统运行的安全性。

7.报表统计：统计各类资源的用户使用量、每类资源的使用情况，如业务系统的CPU、内存、存储、IP的资源总量及占用量。按照天、周、月、季度的频率周期性生成报表。

8.操作系统维护：更新操作系统的系统补丁，清理冗余日志，不定期测试系统性能等。

4.3.2.1.2.3.1.2例行巡检

提供定期巡检服务。制定应用功能例行巡检方案，针对性能容量、可用性、可连续性、可管理性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现软件系统的故障异常、软件告警、潜在问题、安全隐患等，并及时作出适当的处置，保障软件系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够7×24小时正常运行。

定期对应用程序进行例行巡检。同时利用已有监控系统，按照标准规范要求进行监控操作，密切注意软件系统情况。检查过程中同步记录运

行数据，如若发现任何异常情况应及时进行登记，及时通知相关人员进行处理并跟进处理情况，每月形成巡检报告。

例行巡检主要包括以下内容：

1.日常检查

- 1) 应用服务运行情况；
- 2) 日志是否有报错信息；
- 3) 备份配置文件；
- 4) 备份重要运行日志；
- 5) 清除过期日志；
- 6) 系统数据库运行状态；
- 7) 系统主要进程运行状态。

2.性能检查

- 1) 业务CPU使用峰值情况；
- 2) 业务内存使用峰值情况；
- 3) 业务会话连接数情况

3.脆弱性检查

- 1) 重要运行程序是否有保留备份；
- 2) 系统配置是否符合运行的要求；
- 3) 系统使用资源是否超过预定阈值。

4.应用服务器检查

- 1) 查看当前磁盘空间/文件系统使用率、空闲空间情况，查看各挂载点使用及剩余空间；
- 2) 查看当前CPU使用率，内存使用情况，查看当前系统资源消耗情况；
- 3) 查看系统监听的端口，端口能否通畅。

5.系统业务检查

- 1) 通过进程及日志，查看应用后台进程，查看程序进程是否存在；
- 2) 通过页面拨测，检查功能模块。

6.系统数据库服务器检查

- 1) 查看服务器磁盘空间，检查磁盘剩余空间；
- 2) 查看备份作业，检查作业操作历史记录是否正常；
- 3) 查看表空间占用率，磁盘空间>90%发告警；
- 4) 查看临时表空间占用率，磁盘空间>90%发告警。

4.3.2.1.2.3.1.3技术支持

提供7×24小时技术服务，通过现场服务、远程服务以及热线电话等方式，对资讯库的日常咨询、故障问题、专项任务、数据统计、服务投诉等服务请求进行登记，根据事件的性质、类别、等级进行判断，分派相关人员进行处理，并对事件处理全流程进行跟踪监督，确保服务请求得到及时的响应与处理。技术支持服务内容包括：

1.远程服务：在运维服务期阶段，针对出现的系统故障，技术人员将远程进行故障的快速修复，保障系统正常运行。

2.现场服务：在运维服务期阶段，现场服务包括专家保障人员的现场服务、系统故障出现时的现场服务（用户认为有必要到现场）、重大节假日及重要事件或特殊演示现场服务、特殊、重大报道期间的现场服务。针对不同的现场服务内容派出不同专业的经验丰富的技术人员，服务内容包括但不限于现场咨询、故障维修、产品或系统升级、特殊演示等。

3.服务电话：在运维服务期阶段，安排技术支持工程师提供技术支持，提供7×24小时服务电话。

4.电子邮件：可以通过电子邮件将技术支持请求发送到运维服务组，技术人员在接到报告之后，会立即与项目单位取得联系，为其提供相应的技术支持服务。服务团队也将通过电子邮件为项目单位提供解决方案，或者根据业务系统需要发送相关的技术资料。

4.3.2.1.2.3.1.4故障处理

提供故障处理服务。当发生故障时，按照故障定级和处理流程，及时响应，快速抢通故障点，尽早恢复业务，将故障对业务所造成的负面影响降到最低。在处理完毕后清理现场，提供故障处理简报。具体故障处理如下：

- 1.应用软件出现无法启动软件可执行文件时，提前做好各类需维护软件安装程序，将应用软件数据文件备份后，重新安装。
- 2.应用软件打开过程中或运行中异常错误关闭，准备好安装程序，操作系统优化和修补软件，查杀病毒软件，判断出错原因，备份数据，采取相关修复措施。
- 3.操作系统出现系统异常或系统资源占用严重，应准备好系统检查程序及修补程序，以及查杀病毒软件，告知使用者错误原因可能类型，提出解决方案，经使用者认可后采取相应措施。
- 4.操作系统为B/S结构系统，浏览器异常或无法下载控件，准备修复浏览器软件、查杀病毒软件，检查浏览器选项设置，分析原因进行修复。
- 5.账号密码登录错误，检查账号密码是否有错误或重新分配。
- 6.系统未响应或无法访问，关闭系统，重新访问；检查系统访问地址是否有误，网络是否正常，端口是否正常，服务器是否正常开启。
- 7.系统反应缓慢，检测机器性能是否因过低而引起。
- 8.系统端口或数据库端口不通，检测端口是否被占用，更换端口。

4.3.2.1.2.3.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.2.4赋能中心(公众服务窗口、一体化审批)

4.3.2.1.2.4.1一体化审批平台运维服务

运维内容包括针对一体化审批平台的日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.2.4.1.1服务内容

4.3.2.1.2.4.1.1.1日常维护

提供日常维护服务。制定应用功能日常维护方案，针对系统进程、系统接口、系统权限、系统资源、业务保障等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，周期性开展常规维护保养工作，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够7×24小时正常运行。维护对象包括但不限于应用程序、操作系统等。同时按照标准规范对软件系统进行管理，定期形成系统运行简报。具体维护内容如下：

- 1.业务维护：利用管理员账号登录系统查看系统操作日志，监控是否有非法的数据删除、异常登入、登出操作等信息。定期查看系统日志，操作日志，判断是否有运行错误信息，定期备份日志等操作。
- 2.访问管理：系统的用户管理服务，包括：用户账户、权限、组织架构的新增、变更、删除。依据流程分配软件系统的账号和权限，权限以最小原则分配，并对登录日志和权限进行定期审查。根据接入管理的标准规范，设置密码复杂度和登录次数限制等规则。
- 3.软件版本升级：进行软件版本的维护服务前，制定维护方案和回退方案，方案通过审核后，通过服务提供商的技术支持进行维护操作，进行简单流程的变更，并协助用户下载系统应用的补丁程序及软件升级程序，及时协助或提供安装升级服务，不涉及开发和调测等。完成软件版本的维护服务后应出具相应的版本说明。
- 4.日志管理：对软件系统的日志采集、展现和检查分析。日志展现围绕资源的整个生命周期，体现资源的具体操作、操作时间、操作人、操作结果等信息。通过对系统日志进行巡查、抽查和定向检查，提早发现执行路径异常、参数和性能异常。
- 5.配置管理：使软件系统各种配置信息得到有效、完整、可追溯的记录归档和维护。配置信息包括：软件系统及其运行环境中相关的IT设备、系统及其配置信息；各IT设备、系统之间的物理和逻辑关系。
- 6.安全加固：根据测评有关要求，完成应用功能的漏洞修复服务，确保通过相关测评，提升系统运行的安全性。
- 7.系统运行监控服务：对系统的Web日志、应用日志、主机日志的采集、展现和检查分析。提供对被监控的系统运行安全监控与告警展示，提早发现执行路径异常、参数和性能异常。

4.3.2.1.2.4.1.1.2例行巡检

提供定期巡检服务。制定应用功能例行巡检方案，针对性能容量、可用性、可连续性、可管理性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现软件系统的故障异常、软件告警、潜在问题、安全隐患等，并及时作出适当的处置，保障软件系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够7×24小时正常运行。

定期对应用程序进行例行巡检。同时利用已有监控系统，按照标准规范要求进行监控操作，密切注意软件系统情况。检查过程中同步记录运行数据，如若发现任何异常情况应及时进行登记，及时通知相关人员进行处理并跟进处理情况，每月形成巡检报告。

例行巡检主要包括以下内容：

1.日常检查

- 1) 应用服务运行情况；
- 2) 日志是否有报错信息；
- 3) 备份配置文件；
- 4) 备份重要运行日志；
- 5) 清除过期日志；
- 6) 交易连接正常性测试；
- 7) 系统数据库运行状态；
- 8) 系统主要进程运行状态。

2.性能检查

- 1) 业务CPU使用峰值情况；
- 2) 业务内存使用峰值情况；
- 3) 业务会话连接数情况

3.脆弱性检查

- 1) 重要运行程序是否有保留备份；
- 2) 系统配置是否符合运行的要求；
- 3) 系统使用资源是否超过预定阈值。

4.应用服务器检查

- 1) 查看当前磁盘空间/文件系统使用率、空闲空间情况，查看各挂载点使用及剩余空间；
- 2) 查看当前CPU使用率，内存使用情况，查看当前系统资源消耗情况；
- 3) 查看系统监听的端口，端口能否通畅。

5.系统业务检查

- 1) 通过进程及日志，查看应用后台进程，查看程序进程是否存在；
- 2) 通过页面拨测，检查功能模块。

4.3.2.1.2.4.1.1.3技术支持

1.协助开展一体化审批平台组件测试和部署、新监控对象接入调试等工作。在有新的应用系统需要接入系统时，提供新监控对象接入调试服务，配置网络流量采集系统、主机日志采集系统，使得新的监控对象纳入系统的监控监测。

2.对一体化审批平台提供改造服务，针对应用系统的代码功能缺陷，或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求，提供系统迭代服务。

3.提供系统优化服务，主要涉及对应用程序进行代码级别的优化、数据库查询效率的提升、用户界面的改进以及功能的适应性增强等方面。

4.针对系统中各类查询统计报表功能的完善、调整、配置及维护。主要对存在特殊要求的且系统已有查询或汇总分析功能不满足统计分析需求的，提供技术分析、数据辅助查询、安全事件建模、数据关联输出等技术支持服务。

5.在两会、国庆或网络安全重点保障期间，保障一体化审批平台的正常运行，为安全调查分析人员开展网络安全保障监控提供应急支持服务，保障系统的正常运行。

6.根据测评有关要求，完成应用功能的漏洞修复服务，确保通过相关测评，提升系统运行的安全性。

4.3.2.1.2.4.1.1.4故障处理

若系统出现现场运维人员无法解决的问题，根据故障严重程度，采取相应的二线现场支持策略，为系统提供现场故障处理服务。

对于严重故障，需4小时内到达现场，期间保持远程技术支持。到达现场后，4小时内系统恢复运行。需要中标单位配合检查其他影响因素的，4小时内提出解决方案。24小时内系统全部恢复正常。

对于一般故障视情况而定是否现场服务。需在2个工作日内修复故障。

4.3.2.1.2.4.1.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.2.4.2公众统一服务窗口运维服务

4.3.2.1.2.4.2.1服务内容

运维内容包括针对公众统一服务窗口的日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.2.4.2.1.1日常维护

提供日常维护服务。制定应用功能日常维护方案，针对系统进程、系统接口、系统权限、系统资源、业务保障等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，周期性开展常规维护保养工作，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够7×24小时正常运行。维护对象包括但不限于应用程序、操作系统等。同时按照标准规范对软件系统进行管理，定期形成系统运行简报。具体维护内容如下：

1.业务维护：利用管理员账号登录系统查看系统操作日志，监控是否有非法的数据删除、异常登入、登出操作等信息。定期查看系统日志，操作日志，判断是否有运行错误信息，定期备份日志等操作。

2.访问管理：系统的用户管理服务，包括：用户账户、权限、组织架构的新增、变更、删除。依据流程分配软件系统的账号和权限，权限以最小原则分配，并对登录日志和权限进行定期审查。根据接入管理的标准规范，设置密码复杂度和登录次数限制等规则。

3.软件版本升级：进行软件版本的维护服务前，制定维护方案和回退方案，方案通过审核后，通过服务提供商的技术支持进行维护操作，进行简单流程的变更，并协助用户下载系统应用的补丁程序及软件升级程序，及时协助或提供安装升级服务，不涉及开发和调测等。完成软件版本的维护服务后应出具相应的版本说明。

4.日志管理：对软件系统的日志采集、展现和检查分析。日志展现围绕资源的整个生命周期，体现资源的具体操作、操作时间、操作人、操作结果等信息。通过对系统日志进行巡查、抽查和定向检查，提早发现执行路径异常、参数和性能异常。

5.配置管理：使软件系统各种配置信息得到有效、完整、可追溯的记录归档和维护。配置信息包括：软件系统及其运行环境中相关的IT设备、系统及其配置信息；各IT设备、系统之间的物理和逻辑关系。

6、安全加固：根据测评有关要求，完成应用功能的漏洞修复服务，确保通过相关测评，提升系统运行的安全性。

4.3.2.1.2.4.2.1.2例行巡检

提供定期巡检服务。制定应用功能例行巡检方案，针对性能容量、可用性、可连续性、可管理性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现软件系统的故障异常、软件告警、潜在问题、安全隐患等，并及时作出适当的处置，保障软件系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够7×24小时正常运行。

定期对应用程序进行例行巡检。同时利用已有监控系统，按照标准规范要求要求进行监控操作，密切注意软件系统情况。检查过程中同步记录运行数据，如若发现任何异常情况应及时进行登记，及时通知相关人员进行处理并跟进处理情况，每月形成巡检报告。

例行巡检主要包括以下内容：

1.日常检查

1）应用服务运行情况；

2）日志是否有报错信息；

- 3) 备份配置文件;
- 4) 备份重要运行日志;
- 5) 清除过期日志;
- 6) 交易连接正常性测试;
- 7) 数据库运行状态;
- 8) 主要进程运行状态。

2.性能检查

- 1) 业务CPU使用峰值情况;
- 2) 业务内存使用峰值情况;
- 3) 业务会话连接数情况

3.脆弱性检查

- 1) 重要运行程序是否有保留备份;
- 2) 系统配置是否符合运行的要求;
- 3) 系统使用资源是否超过预定阈值。

4.应用服务器检查

- 1) 查看当前磁盘空间/文件系统使用率、空闲空间情况, 查看各挂载点使用及剩余空间;
- 2) 查看当前CPU使用率, 内存使用情况, 查看当前系统资源消耗情况;
- 3) 查看系统监听的端口, 端口能否通畅。

5.系统业务检查

- 1) 通过进程及日志, 查看应用后台进程, 查看程序进程是否存在;
- 2) 通过页面拨测, 检查功能模块。

4.3.2.1.2.4.2.1.3技术支持

1.协助开展系统组件测试和部署、新监控对象接入调试等工作。在有新的应用系统需要接入系统时, 提供新监控对象接入调试服务, 配置网络流量采集系统、主机日志采集系统, 使得新的监控对象纳入系统的监控监测。

2.对公众统一服务窗口提供改造服务, 针对应用系统的代码功能缺陷, 或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求, 提供系统迭代服务。

3.提供业务系统优化服务, 主要涉及对应用程序进行代码级别的优化、用户界面的改进以及功能的适应性增强等方面。

4.针对系统中各类查询统计报表功能的完善、调整、配置及维护。主要针对存在特殊要求的且系统已有查询或汇总分析功能不满足统计分析需求的, 提供技术分析、数据辅助查询、安全事件建模、数据关联输出等技术支持服务。

5.在两会、国庆或网络安全重点保障期间, 保障系统的正常运行, 为安全调查分析人员开展网络安全保障监控提供应急支持服务, 保障系统的正常运行。

6.根据测评有关要求, 完成应用功能的漏洞修复服务, 确保通过相关测评, 提升系统运行的安全性。

4.3.2.1.2.4.2.1.4故障处理

若系统出现现场运维人员无法解决的问题, 根据故障严重程度, 采取相应的二线现场支持策略, 为系统提供现场故障处理服务。

对于严重故障, 需4小时内到达现场, 期间保持远程技术支持。到达现场后, 4小时内系统恢复运行。需要中标单位配合检查其他影响因素的, 4小时内提出解决方案。24小时内系统全部恢复正常。

对于一般故障视情况而定是否现场服务。需在2个工作日内修复故障。

4.3.2.1.2.4.2.2服务成果

系统月度巡检报告;

系统故障处理报告(按需提供);

系统年度运维服务总结报告。

4.3.2.1.2.5赋能中心(用户中心、消息中心、集成门户、数字政府公共能力中心)

4.3.2.1.2.5.1服务内容

对用户中心、消息中心、集成门户、数字政府公共能力中心提供运维服务，包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.2.5.1.1日常维护

对系统提供日常维护服务，主要包括资源管理、权限管理、版本发布管理、功能配置等；建立服务器、存储等资源的全生命周期动态台账，实现负载监控与扩缩容支持的闭环；基于实施账号权限最小化原则，对系统账号权限进行全流程管理，同时，开展账号日志审计与异常权限调整处理工作；遵循非高峰发布、预测试验证、灰度升级（单节点/集群滚动）灰度升级（单节点/集群滚动）等，确保版本迭代工作规范进行；同时提供系统功能配置优化服务，提升系统的业务适配性；形成“资源可溯、权限可控、发布可靠、配置高效”的日常维护模式，确保快速响应，保障系统稳定运行。主要工作内容如下：

4.3.2.1.2.5.1.1.1资源管理

提供资源管理服务，管理系统资源清单台账；梳理系统涉及的各种资源类型，输出包括IP信息、CPU、内存、容量、实例名称、组件版本、用途等关键信息，实现对云主机、存储资源的精细化管理跟踪，确保资源纳入规范化监控，做好资源变动时的清单台账联动更新。协助规划设计云资源负载管理，提供关键技术统计指标，为系统扩缩容提供技术支持。

4.3.2.1.2.5.1.1.2权限管理

提供权限管理服务，遵循最小权限原则与安全审计要求，集中管理运维相关账号，管控运维人员访问权限，仅允许授权人员通过可信网络接入；定期复核权限分配策略，调整权限、处理闲置账号，确保与安全管理要求一致；记录留存运维过程中的会话日志，支持事后追溯与合规审查。每月审查账号权限，确保符合最小权限原则和安全政策；审查操作系统关键角色权限、中间件权限、非结构化存储权限等，定期更新账号密码，保障系统及数据安全。系统变更或业务需求变化时，及时调整基础软件角色权限，保证时效性和准确性，支撑运维工作。低权限用户联调或排错需提权时，进行临时赋权，操作完成后及时回收权限，遵循最小权限原则。根据用户状态更新或回收账号，如账号所有者离场时回收其权限。

对应用账号建立覆盖全生命周期管理体系，包括账号的规范化创建、权限动态调整、离职/转岗账号冻结或注销等流程。按角色、业务场景精细化授权，确保权限最小化原则，避免越权访问。需定期开展账号权限审计，核查冗余账号、异常权限分配（如超管权限滥用），针对临时账号（如等保测评、密评等）需建立审批流程与时限控制机制，防范权限泄漏风险。

4.3.2.1.2.5.1.1.3系统版本发布

提供系统版本发布服务；如用户管理模块、消息订阅模块以及通用配置模块等需要迭代更新时，需要按照规范化开展版本更新工作；具体包括需要制定版本规划，版本发布后需完成相关测试，验证相关功能是否满足迭代目标；若验证不通过，需要将新版本回退到原有版本。主要流程如下：

1、发布版本规划：确定发布计划，包括日期、内容、范围、方式、流程步骤、任务、责任人及时间节点等；确定发布时间，综合考量业务需求等因素，选在业务低峰期；制定备份策略，对系统文件、配置文件、数据库进行全量备份。

2、发布版本申请：按变更管理规范流程申请变更，审核人审核版本变更目标、时间计划、影响范围、风险评估及应对措施。

3、执行版本发布：单节点升级时，停止服务、执行升级、更新配置文件、启动服务并验证状态；集群滚动升级分批进行，通过负载均衡器路由流量；分布式系统升级分阶段进行，避免服务中断；功能验证时测试验证系统核心功能，检查日志及监控指标。发布测试验证不通过时，停止新版本服务，从备份恢复旧版本及配置文件，记录回滚原因及操作步骤，生成回滚报告。

4、系统更新后全链路验证：针对版本升级或配置调整，模拟真实用户操作路径，覆盖核心业务流程，验证功能完整性与业务连续性；开展高并发、异常场景压力测试，确保系统稳定性与容错能力。

5、持续监控与效果闭环：优化后通过AB测试、用户回访验证效果，确保版本发布后问题解决率达标。建立用户体验指标体系（操作成功率、响应时间），长效跟踪系统使用情况。

4.3.2.1.2.5.1.1.4日常功能配置

提供日常功能配置服务，包括但不限于流程节点规则调整、表单字段增删、审批层级变更、系统进程配置优化等。针对高频配置场景，需提供模板化配置工具，提升效率并降低人工操作风险。所有配置操作需留存完整日志，支持事后追溯审计。

4.3.2.1.2.5.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行；基于服务器、数据库、容器等基础资源及核心业务功能（如接口成功率、响应时间）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

4.3.2.1.2.5.1.2.1系统监控

1、提供基础环境监控服务，梳理运行环境监控对象及对应监控指标，明确取数频次和计算方式，实现精确监控。制定监控告警策略和级别管理，调整指标基线，明确告警阈值，针对问题收敛优化策略，确保有效预警。部署、调试监控采集器并维护，保障监控数据有效可靠。然后实时监控服务器、数据库、TKE等基础资源使用情况，如CPU使用率、内存使用率、磁盘空间使用率、I/O速率等指标，触发告警时及时响应处理，必要时转二线升级处理并跟踪进度。针对发现的告警进行根因分析，响应处理监控告警信息，解决故障问题并详细记录；定期收集分析监控数据，提出告警策略优化建议。

2、提供业务功能监控服务，针对核心业务功能实施监控，如集成门户、用户中心、消息中心等重要页面接口实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

4.3.2.1.2.5.1.2.2系统巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，页面响应时间>1000ms告警。

4.3.2.1.2.5.1.3技术支持

对系统提供技术支持服务，主要包括以下内容：通过标准化变更流程（需求评估、灰度发布、回滚验证）与配置管理数据库动态维护，保障系统变更可追溯、风险可控；围绕安全漏洞修复（版本升级、基线加固、弱密码整改）等保测评合规改造，提升系统抗风险能力；针对性能瓶颈开展架构调优（容器资源弹性扩缩、微服务链路治理），结合全链路压测验证效能提升；建立应急重保专班，按预案执行故障隔离、资源调配及快速恢复，完善“演练—处置—复盘”闭环；同步支撑功能配置动态调整、数据完整性维护及用户问题实时响应，形成“事前预防—事中控制—事后优化”的一体化响应体系，确保系统稳定性、安全性与业务连续性高效协同。具体服务内容如下：

4.3.2.1.2.5.1.3.1变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、数据增删改、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求提请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

（2）变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。

（3）变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。

（4）变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

4.3.2.1.2.5.1.3.2配置管理

提供配置管理服务，规范整个系统的配置管理流程。建立和维护标准化、系统化的配置管理台账，确保所有配置项都得到记录和控制。配置管理的服务内容如下：

- （1）配置关系梳理：确认配置范围、定义和标识配置项，梳理关联关系，制定配置管理机制、变更与审核流程机制、文档管理机制，形成体系化配置管理数据库。
- （2）配置数据录入：明确配置管理数据库所需配置信息和清单，录入配置项信息，确保准确性、适用性和可维护性。
- （3）配置数据更新：根据系统版本发布和变更情况，发起配置任务，更新配置库环境和调整配置基线；建立定期审查计划，排查与实际情况不匹配的情况；定期备份配置库，防止数据丢失。

4.3.2.1.2.5.1.3.3系统安全管理

提供系统安全管理服务，规范系统安全风险从接收、整改到验证的整个流程，具体服务内容如下：

- （1）安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。
- （2）安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。
- （3）安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。
- （4）整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。
- （5）整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改问题报告。

4.3.2.1.2.5.1.3.4应急与重保统筹组织

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

- （1）应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。
- （2）应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。
- （3）应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。
- （4）应急与重保支持：定期组织应急重保支持，模拟不同应急场景，验证预案可行性和团队协作效率，记录薄弱环节以便优化。
- （5）应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

4.3.2.1.2.5.1.3.5系统优化

提供系统优化服务，优化主要包括两部分，一是运行环境优化，对系统的基础架构进行调整和改进，以确保系统能够更加高效、稳定地运行，这包括但不限于硬件资源的合理分配、操作系统级别的性能调优、以及网络环境的优化等。二是应用优化，主要涉及对应用程序进行代码级别的优化、用户界面的改进以及功能的适应性增强等方面。通过这两部分的优化，可以显著提高系统的整体性能，确保用户能够获得更加流畅和高效的使用体验。

（1）针对基础软件运行架构的缺陷，或由于故障、安全等要求提出的需求，对系统运行架构环境进行调优与完善，提升应用的响应速度。运行架构调整与优化工作包括数据库优化、容器优化、操作系统参数优化调整等。

TKE优化调整：检查TKE部署组服务状态、针对资源不足或存在性能卡点的服务进行调整优化；如调整资源分配、副本数、以及启用弹性伸缩容策略等；优化网络配置与存储类型、通过监控工具定位瓶颈，针对性调优服务配置。

服务器优化调整：清理无用文件与进程释放资源，调整内核参数，优化磁盘I/O，升级系统补丁，关闭非必要服务降低资源占用。

（2）提供应用架构与性能优化服务，对系统在高并发、大数据量场景下的性能瓶颈（如接口超时、数据库慢查询），提出应用优化方案，包括但不限于缓存策略调整、SQL优化、异步任务拆分、连接池调整等。确保关键应用服务响应时间符合业务要求，优化后需提供基准测试结果对比，量化性能提升效果。

首先，调研系统实际运行场景，梳理高并发、大数据量业务环节，明确性能评估重点。搭建贴近生产环境的测试环境，模拟实际业务流量，对系统进行压力测试与性能基准测试，精准定位性能瓶颈。借助专业性能分析工具，对系统运行数据进行全方位剖析，涵盖服务器资源使用情况、数据库查询日志、接口调用链路等，深入挖掘性能瓶颈根源。

基于性能评估结果，结合系统业务特点和未来发展规划，制定针对性的架构优化方案，包括但不限于异步任务重构、微服务架构适配等。制定详细计划，逐步推进架构与代码优化，确保业务不受影响；遵循规范与版本控制，严格审查与测试代码；优化后进行压力与基准测试，对比性能指标，验证方案有效性。根据性能验证结果，编制详细的基准测试对比报告，以数据与图表展示性能提升，如响应时间缩短、查询效率提高、吞吐量增加。对性能提升效果进行深入分析，阐述优化方案对政务软件系统的实际影响，提供客观、准确的性能评估依据。

4.3.2.1.2.5.1.3.6安全加固

提供系统安全加固服务，包括基础环境和应用系统两个方面的加固，以确保整个系统的安全性和稳定性。基础环境加固通常包括操作系统、数据库等配置优化，以减少潜在的安全漏洞，涉及更新系统补丁、关闭不必要的服务端口、配置防火墙规则以及实施严格的访问控制策略；业务应用加固则侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

（1）基础环境加固：对基础软件运行环境进行安全加固，根据日常安全监控、测评、定期漏洞等发现的基础环境安全问题，先对漏洞问题进行分析，再通过限制访问、升级补丁等方式进行加固修复工作，修复前先需要先进行测试验证，避免修复过程中出现服务异常、重启失败等次生问题，遵循规范的变更管理流程进行漏洞修复工作。此外，基础环境安全加固还包括对重要基础软件进行定向升级、配置基线加固、配合审计工作或进行符合性安全改造等工作。主要包括以下内容：

基础软件版本升级：检查升级操作系统、中间件至最稳定版本，进行版本升级、病毒库更新等；优先通过官方补丁修复漏洞，针对无法直接修复的漏洞通过配置调整或第三方组件替换规避，清理冗余日志。

基础软件安全基线加固：结合系统安全需求制定基础软件安全基线，涵盖各项安全配置要求，组织专家评审确认基线合理性、完整性和可操作性。利用工具或手动方式检查调整基础软件配置，使其符合安全基线；定期复查安全配置，整改修复不符合项。

弱密码整改：明确密码设置规范，定期排查系统弱密码，提醒用户修改；新用户注册严格审核密码合规性。

网络策略收敛：按照网络安全管理策略，分析现有网络访问规则，识别冗余、冲突或过宽权限，收敛至最小必要访问原则，降低攻击面。

配合审计工作或进行符合性安全改造：梳理与安全审计相关的业务流程和数据流向，明确关键操作和事件，评估现有审计日志功能，制定改进方案。依据需求分析结果，完善基础软件审计功能，配合安全审计团队工作，提供技术支持与数据协助，整改发现的问题，确保符合安全审计要求。

等保测评工作配合及符合性改造：根据等保要求调整系统配置，配合测评机构完成系统定级、差距分析、整改验证等工作。涵盖技术改造与管理改造，技术上针对等保标准进行系统加固，管理上完善安全制度、明确责任与流程，定期开展安全培训。

（2）应用安全加固服务，针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固；如越权访问、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

4.3.2.1.2.5.1.3.7备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日

志分析及及时提供技术支持，确保备份策略正常运行。

4.3.2.1.2.5.1.3.8业务支持

面向系统用户提供业务支持，提升用户在使用软件系统推进业务时的体验，在遇到疑问时能够及时获得相应的指引与建议。

4.3.2.1.2.5.1.4故障处理

对系统提供故障处理服务，以快速响应、精准定位、闭环管理为核心，构建覆盖“接收—分级—处置—验证—复盘”的规范化故障处理机制：通过监控告警、用户上报等多渠道接收故障，按业务影响分级响应，分派至对应团队紧急处置（如操作系统内核修复、数据库一致性恢复、中间件配置调优、网络拓扑排查及应用层服务重启等），结合日志分析、链路追踪定位根因，实施代码修复、环境回滚或资源扩容等方案；处置后通过全链路验证（功能、性能、数据一致性）确认恢复，释放临时资源并标准化配置；同步启动问题管理，对未根治故障及潜在缺陷进行根因分析，形成《问题报告》并沉淀至知识库，优化应急预案与监控策略；针对应用BUG，严格遵循“环境复现—测试验证—灰度发布”流程，确保修复代码安全上线，最终通过跨团队协作与经验复用，实现故障响应时效、修复质量及系统健壮性的三重提升，降低同类问题复发风险。故障处理工作主要包括以下具体工作内容：

4.3.2.1.2.5.1.4.1故障管理

整合故障反馈渠道，安排专人通过监控告警、巡检识别或用户上报等渠道发现接收故障需求，记录故障情况。一是初步识别故障，判断类型和影响范围，按业务重要性和影响范围划分故障等级和处置优先级。二是根据故障级别和类型，分派任务至对应运维人员处理，依据机制向相关人员通报故障情况和进度，记录时间节点。三是深入分析故障，制定处置方案，经领导同意后按职责实施处置。四是故障处理结束后，验证处理结果，检查系统运行情况和关键指标是否恢复正常，若未根本解决则记录信息和意见，触发问题解决与管理及变更管理流程。五是若处理过程中涉及临时增加资源的，需在完成故障处理闭环后，删除临时文件，释放系统资源，恢复配置或策略至标准状态，避免二次故障。涉及重大故障的，需在故障修复一周内，总结故障经验形成《系统故障处理报告》，同时对重大故障启动复盘会议，优化应急预案和监控策略。

4.3.2.1.2.5.1.4.2问题管理

收集问题途径包括未根本解决的故障、日常巡检与监控告警、日志分析等，详细记录问题情况。判断问题类型与影响范围，组织技术专家联合进行根因分析，明确是否为已知错误或新发缺陷，提出处置与改进建议。根据建议制定处理计划，验证可行性后严格执行，防止故障再次发生和引入二次风险。问题发起方验证处理结果，确认解决且无副作用，比对运维基线数据，记录验证结果于《问题报告》。复盘分析问题根本原因，探讨从运维管理、系统架构设计、技术选型等方面优化，避免类似问题再次发生，沉淀为运维知识库案例。关闭前核对处理记录、验证结果及相关文档完整性，经双方签字确认；涉及配置修改或软件升级时，需变更管理流程审批，实施后回归测试确保未复发。

4.3.2.1.2.5.1.4.3应用缺陷修复

依据缺陷描述搭建与生产环境高度一致的测试环境，依照操作步骤执行复现，详细记录操作及系统响应，形成复现报告。运用工具和日志分析，结合复现报告定位代码错误位置和逻辑错误，深入剖析原因及对其他模块的影响。按修复方案进行代码修改，开展单元测试、集成测试、系统测试，验证修复后代码的正确性、集成情况及系统稳定性可靠性。制定发布计划，对修复代码打包部署前检查，按计划在生产环境发布，发布过程中监控系统运行状态，发布后验证并收集用户反馈。

4.3.2.1.2.5.1.4.4常见故障处理

（1）操作系统故障处理：检查系统日志、系统内核参数配置、安全策略配置、驱动程序异常等，深入分析故障原因，采取相应解决措施，如更新或回滚驱动程序、修复替换损坏文件等；修复后进行稳定性测试，确保系统恢复正常且无新问题。

（2）中间件故障处理：查看中间件运行日志、性能指标、连接状态、配置文件等，判断故障原因，采取相应解决措施；处理完成后进行全面功能和性能测试，验证中间件及业务功能恢复正常。

（3）系统网络故障处理：接到故障报告后启动排查流程，梳理网络拓扑结构，对端口抓包确定故障位置和范围。

（4）应用故障处理：在系统发生故障时（如服务不可用、页面卡顿、服务调用异常等）需及时响应，优先通过应用层配置调整恢复业务；通过日志分析、链路追踪等手段定位根因，并要输出故障分析报告，故障排除后需要进行复盘，并提出相应的改进措施纳入应急预案；建立常见故障知识库，降低同类问题复发概率。

4.3.2.1.2.5.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.2.6赋能中心(信息资源管理中心)

4.3.2.1.2.6.1服务内容

对系统的信息资源管理、信息资源调度、信息资源监控、云专区监控接入、日志中心、信息资源门户等模块提供日常维护、例行巡检、技术支持、故障处理等服务。

4.3.2.1.2.6.1.1日常维护

对系统提供日常维护服务，包括资源管理、权限管理、版本发布管理、功能配置等，建立服务器、存储等资源的全生命周期动态台账，实现负载监控与扩缩容支持的闭环；基于实施账号权限最小化原则，对系统账号权限进行全流程管理，同时，开展账号日志审计与异常权限调整处理工作；遵循非高峰发布、预测试验证、灰度升级（单节点/集群滚动）灰度升级（单节点/集群滚动）等，确保版本迭代工作规范进行；同时提供系统功能配置优化服务，提升系统的业务适配性；形成“资源可溯、权限可控、发布可靠、配置高效”的日常维护模式，确保快速响应，保障系统稳定运行。日常维护主要工作内容如下：

4.3.2.1.2.6.1.1.1资源管理

提供资源管理服务，管理系统资源清单台账；梳理系统涉及的各种资源类型，输出包括IP信息、CPU、内存、容量、实例名称、组件版本、用途等关键信息，实现对云主机、存储、数据库等资源的精细化管理跟踪，确保资源纳入规范化监控，做好资源变动时的清单台账联动更新。协助规划设计云资源负载管理，提供关键技术统计指标，为系统扩缩容提供技术支持。

4.3.2.1.2.6.1.1.2权限管理

提供权限管理服务，遵循最小权限原则与安全审计要求，集中管理运维相关账号，管控运维人员访问权限，仅允许授权人员通过可信网络接入；定期复核权限分配策略，调整权限、处理闲置账号，确保与安全管理要求一致；记录留存运维过程中的会话日志，支持事后追溯与合规审查。每月审查账号权限，确保符合最小权限原则和安全政策；审查操作系统关键角色权限、数据库权限、中间件权限、非结构化存储权限等，定期更新账号密码，保障系统及数据安全。系统变更或业务需求变化时，及时调整基础软件角色权限，保证时效性和准确性，支撑运维工作。低权限用户联调或排错需提权时，进行临时赋权，操作完成后及时回收权限，遵循最小权限原则。根据用户状态更新或回收账号，如账号所有者离场时回收其权限。

对应用账号建立覆盖全生命周期管理体系，包括账号的规范化创建、权限动态调整、离职/转岗账号冻结或注销等流程。按角色、业务场景精细化授权，确保权限最小化原则，避免越权访问。需定期开展账号权限审计，核查冗余账号、异常权限分配（如超管权限滥用），针对临时账号（如等保测评、密评等）需建立审批流程与时限控制机制，防范权限泄漏风险。

4.3.2.1.2.6.1.1.3系统版本发布

提供系统版本发布服务，当应用程序版本需要更新时，需要对新版本的软件系统发布进行规划，且需完成相关测试，验证新版本软件系统能够正常运行，才能进行正式的发布。若验证不通过，需要将新版本回退到原有版本。主要流程如下：

1、发布版本规划：确定发布计划，包括日期、内容、范围、方式、流程步骤、任务、责任人及时间节点等；确定发布时间，综合考量业务需求等因素，选在业务低峰期；制定备份策略，对系统文件、配置文件、数据库进行全量备份。

2、发布版本申请：按变更管理规范流程申请变更，审核人审核版本变更目标、时间计划、影响范围、风险评估及应对措施。

3、执行版本发布：单节点升级时，停止服务、执行升级、更新配置文件、启动服务并验证状态；集群滚动升级分批进行，通过负载均衡器路由流量；分布式系统升级分阶段进行，避免服务中断；功能验证时测试验证系统核心功能，检查日志及监控指标。发布测试验证不通过时，停止新版本服务，从备份恢复旧版本及配置文件，记录回滚原因及操作步骤，生成回滚报告。

4、系统更新后全链路验证：针对版本升级或配置调整，模拟真实用户操作路径，覆盖核心业务流程，验证功能完整性与业务连续性；开展高并发、异常场景压力测试，确保系统稳定性与容错能力。

5、持续监控与效果闭环：优化后通过AB测试、用户回访验证效果，确保版本发布后问题解决率达标。建立用户体验指标体系（操作成功率、响应时间），长效跟踪系统使用情况。

4.3.2.1.2.6.1.1.4日常功能配置

提供日常功能配置服务，包括但不限于流程节点规则调整、表单字段增删、审批层级变更、系统进程配置优化等。针对高频配置场景，需提供模板化配置工具，提升效率并降低人工操作风险。所有配置操作需留存完整日志，支持事后追溯审计。

4.3.2.1.2.6.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：基于服务器、容器等基础资源及核心业务功能（如接口成功率、响应时间）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

4.3.2.1.2.6.1.2.1系统监控

1、提供基础环境监控服务，梳理运行环境监控对象及对应监控指标，明确取数频次和计算方式，实现精确监控。制定监控告警策略和级别管理，调整指标基线，明确告警阈值，针对问题收敛优化策略，确保有效预警。部署、调试监控采集器并维护，保障监控数据有效可靠。然后实时监控服务器、数据库、容器等基础资源使用情况，如CPU使用率、内存使用率、磁盘空间使用率、I/O速率等指标，触发告警时及时响应处理，必要时转二线升级处理并跟踪进度。针对发现的告警进行根因分析，响应处理监控告警信息，解决故障问题并详细记录；定期收集分析监控数据，提出告警策略优化建议。

2、提供业务功能监控服务，针对核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

4.3.2.1.2.6.1.2.2系统巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，页面响应时间>1000ms告警。

4.3.2.1.2.6.1.3技术支持

对系统提供技术支持服务，主要包括以下内容：通过标准化变更流程（需求评估、灰度发布、回滚验证）与配置管理数据库动态维护，保障系统变更可追溯、风险可控；围绕安全漏洞修复（版本升级、基线加固、弱密码整改）等保测评合规改造，提升系统抗风险能力；针对性能瓶颈开展架构调优（数据库SQL优化、容器资源弹性扩缩、微服务链路治理），结合全链路压测验证效能提升；建立应急重保专班，按预案执行故障隔离、资源调配及快速恢复，完善“演练—处置—复盘”闭环；同步支撑功能配置动态调整、数据完整性维护及用户问题实时响应，形成“事前预防—事中控制—事后优化”的一体化响应体系，确保系统稳定性、安全性与业务连续性高效协同。具体服务内容如下：

4.3.2.1.2.6.1.3.1变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求提请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

（2）变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。

（3）变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。

(4) 变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

4.3.2.1.2.6.1.3.2配置管理

提供配置管理服务，规范整个系统的配置管理流程。建立和维护标准化、系统化的配置管理台账，确保所有配置项都得到记录和控制。配置管理的服务内容如下：

(1) 配置关系梳理：确认配置范围、定义和标识配置项，梳理关联关系，制定配置管理机制、变更与审核流程机制、文档管理机制，形成体系化配置管理数据库。

(2) 配置数据录入：明确配置管理数据库所需配置信息和清单，录入配置项信息，确保准确性、适用性和可维护性。

(3) 配置数据更新：根据系统版本发布和变更情况，发起配置任务，更新配置库环境和调整配置基线；建立定期审查计划，排查与实际情况不匹配的情况；定期备份配置库，防止数据丢失。

4.3.2.1.2.6.1.3.3系统安全管理

提供系统安全管理服务，规范系统安全风险从接收、整改到验证的整个流程，具体服务内容如下：

(1) 安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。

(2) 安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。

(3) 安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。

(4) 整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。

(5) 整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改问题报告。

4.3.2.1.2.6.1.3.4应急与重保统筹组织

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

(1) 应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。

(2) 应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。

(3) 应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。

(4) 应急与重保支持：定期组织应急重保支持，模拟不同应急场景，验证预案可行性和团队协作效率，记录薄弱环节以便优化。

(5) 应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

4.3.2.1.2.6.1.3.5系统优化

提供系统优化服务，优化主要包括两部分，一是运行环境优化，对系统的基础架构进行调整和改进，以确保系统能够更加高效、稳定地运行，这包括但不限于硬件资源的合理分配、操作系统级别的性能调优、以及网络环境的优化等。二是应用优化，主要涉及对应用程序进行代码级别的优化、数据库查询效率的提升、用户界面的改进以及功能的适应性增强等方面。通过这两部分的优化，可以显著提高系统的整体性能，确保用户能够获得更加流畅和高效的使用体验。

(1) 针对基础软件运行架构的缺陷，或由于故障、安全等要求提出的需求，对系统运行架构环境进行调优与完善，提升应用的响应速度。运行架构调整与优化工作包括数据库优化、容器优化、操作系统参数优化调整等。

容器优化调整：检查TKE集群节点、Pod状态等，扩容节点资源或调整Pod资源限制，启用弹性扩缩容策略；优化网络配置与存储类型；通过监控工具定位瓶颈，针对性调优服务配置。

服务器优化调整：清理无用文件与进程释放资源，调整内核参数，优化磁盘I/O，升级系统补丁，关闭非必要服务降低资源占用。

(2) 提供应用架构与性能优化服务，对系统在高并发、大数据量场景下的性能瓶颈（如接口超时、数据库慢查询），提出应用优化方案，包括但不限于缓存策略调整、SQL优化、异步任务拆分、连接池调整等。确保关键应用服务响应时间符合业务要求，优化后需提供基准测试结果对

比，量化性能提升效果。

首先，调研系统实际运行场景，梳理高并发、大数据量业务环节，明确性能评估重点。搭建贴近生产环境的测试环境，模拟实际业务流量，对系统进行压力测试与性能基准测试，精准定位性能瓶颈。借助专业性能分析工具，对系统运行数据进行全方位剖析，涵盖服务器资源使用情况、数据库查询日志、接口调用链路等，深入挖掘性能瓶颈根源。

基于性能评估结果，结合系统业务特点和未来发展规划，制定针对性的架构优化方案，包括但不限于异步任务重构、微服务架构适配等。制定详细计划，逐步推进架构与代码优化，确保业务不受影响；遵循规范与版本控制，严格审查与测试代码；优化后进行压力与基准测试，对比性能指标，验证方案有效性。根据性能验证结果，编制详细的基准测试对比报告，以数据与图表展示性能提升，如响应时间缩短、查询效率提高、吞吐量增加。对性能提升效果进行深入分析，阐述优化方案对政务软件系统的实际影响，提供客观、准确的性能评估依据。

4.3.2.1.2.6.1.3.6安全加固

提供系统安全加固服务，包括基础环境和应用系统两个方面的加固，以确保整个系统的安全性和稳定性。基础环境加固通常包括操作系统等配置优化，以减少潜在的安全漏洞，涉及更新系统补丁、关闭不必要的服务端口、配置防火墙规则以及实施严格的访问控制策略；业务应用加固则侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

（1）基础环境加固：对基础软件运行环境进行安全加固，根据日常安全监控、测评、定期漏洞等发现的基础环境安全问题，先对漏洞问题进行分析，再通过限制访问、升级补丁等方式进行加固修复工作，修复前先需要先行测试验证，避免修复过程中出现服务异常、重启失败等次生问题，遵循规范的变更管理流程进行漏洞修复工作。此外，基础环境安全加固还包括对重要基础软件进行定向升级、配置基线加固、配合审计工作或进行符合性安全改造等工作。主要包括以下内容：

基础软件版本升级：每月检查升级操作系统、中间件、数据库至最稳定版本，进行版本升级、病毒库更新等；优先通过官方补丁修复漏洞，针对无法直接修复的漏洞通过配置调整或第三方组件替换规避，清理冗余日志。

基础软件安全基线加固：结合系统安全需求制定基础软件安全基线，涵盖各项安全配置要求，组织专家评审确认基线合理性、完整性和可操作性。利用工具或手动方式检查调整基础软件配置，使其符合安全基线；定期复查安全配置，整改修复不符合项。

弱密码整改：明确密码设置规范，定期排查系统弱密码，提醒用户修改；新用户注册严格审核密码合规性。

网络策略收敛：按照网络安全管理策略，分析现有网络访问规则，识别冗余、冲突或过宽权限，收敛至最小必要访问原则，降低攻击面。

配合审计工作或进行符合性安全改造：梳理与安全审计相关的业务流程和数据流向，明确关键操作和事件，评估现有审计日志功能，制定改进方案。依据需求分析结果，完善基础软件审计功能，配合安全审计团队工作，提供技术支持与数据协助，整改发现的问题，确保符合安全审计要求。

等保测评工作配合及符合性改造：根据等保要求调整系统配置，配合测评机构完成系统定级、差距分析、整改验证等工作。涵盖技术改造与管理改造，技术上针对等保标准进行系统加固，管理上完善安全制度、明确责任与流程，定期开展安全培训。

（2）应用安全加固服务，针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固；如越权访问、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

4.3.2.1.2.6.1.3.7备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略

可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日志分析及时提供技术支持，确保备份策略正常运行。

4.3.2.1.2.6.1.3.8业务支持

面向系统用户提供业务支持，提升用户在使用软件系统推进业务时的体验，在遇到疑问时能够及时获得相应的指引与建议。

4.3.2.1.2.6.1.4故障处理

对系统提供故障处理服务，以快速响应、精准定位、闭环管理为核心，构建覆盖“接收—分级—处置—验证—复盘”的规范化故障处理机制：通过监控告警、用户上报等多渠道接收故障，按业务影响分级响应，分派至对应团队紧急处置（如操作系统内核修复、数据库一致性恢复、中间件配置调优、网络拓扑排查及应用层服务重启等），结合日志分析、链路追踪定位根因，实施代码修复、环境回滚或资源扩容等方案；处置后通过全链路验证（功能、性能、数据一致性）确认恢复，释放临时资源并标准化配置；同步启动问题管理，对未根治故障及潜在缺陷进行根因分析，形成《问题报告》并沉淀至知识库，优化应急预案与监控策略；针对应用BUG，严格遵循“环境复现—测试验证—灰度发布”流程，确保修复代码安全上线，最终通过跨团队协作与经验复用，实现故障响应时效、修复质量及系统健壮性的三重提升，降低同类问题复发风险。故障处理工作主要包括以下具体工作内容：

4.3.2.1.2.6.1.4.1故障管理

整合故障反馈渠道，安排专人通过监控告警、巡检识别或用户上报等渠道发现接收故障需求，记录故障情况。一是初步识别故障，判断类型和影响范围，按业务重要性和影响范围划分故障等级和处置优先级。二是根据故障级别和类型，分派任务至对应运维人员处理，依据机制向相关人员通报故障情况和进度，记录时间节点。三是深入分析故障，制定处置方案，经领导同意后按职责实施处置。四是故障处理结束后，验证处理结果，检查系统运行情况和关键指标是否恢复正常，若未根本解决则记录信息和意见，触发问题解决与管理 and 变更管理流程。五是若处理过程中涉及临时增加资源的，需在完成故障处理闭环后，删除临时文件，释放系统资源，恢复配置或策略至标准状态，避免二次故障。故障修复一周内，总结故障经验形成报告，对重大故障启动复盘会议，优化应急预案和监控策略。

4.3.2.1.2.6.1.4.2问题管理

收集问题途径包括未根本解决的故障、日常巡检与监控告警、日志分析等，详细记录问题情况。判断问题类型与影响范围，组织技术专家联合进行根因分析，明确是否为已知错误或新发缺陷，提出处置与改进建议。根据建议制定处理计划，验证可行性后严格执行，防止故障再次发生和引入二次风险。问题发起方验证处理结果，确认解决且无副作用，比对运维基线数据，记录验证结果于《问题报告》。复盘分析问题根本原因，探讨从运维管理、系统架构设计、技术选型等方面优化，避免类似问题再次发生，沉淀为运维知识库案例。关闭前核对处理记录、验证结果及相关文档完整性，经双方签字确认；涉及配置修改或软件升级时，需变更管理流程审批，实施后回归测试确保未复发。

4.3.2.1.2.6.1.4.3应用缺陷修复

依据缺陷描述搭建与生产环境高度一致的测试环境，依照操作步骤执行复现，详细记录操作及系统响应，形成复现报告。运用工具和日志分析，结合复现报告定位代码错误位置和逻辑错误，深入剖析原因及对其他模块的影响。按修复方案进行代码修改，开展单元测试、集成测试、系统测试，验证修复后代码的正确性、集成情况及系统稳定性可靠性。制定发布计划，对修复代码打包部署前检查，按计划在生产环境发布，发布过程中监控系统运行状态，发布后验证并收集用户反馈。

4.3.2.1.2.6.1.4.4常见故障处理

（1）操作系统故障处理：检查系统日志、系统内核参数配置、安全策略配置、驱动程序异常等，深入分析故障原因，采取相应解决措施，如更新或回滚驱动程序、修复替换损坏文件等；修复后进行稳定性测试，确保系统恢复正常且无新问题。

（2）中间件故障处理：查看中间件运行日志、性能指标、连接状态、配置文件等，判断故障原因，采取相应解决措施；处理完成后进行全面功能和性能测试，验证中间件及业务功能恢复正常。

（3）系统网络故障处理：接到故障报告后启动排查流程，梳理网络拓扑结构，对端口抓包确定故障位置和范围。

（4）应用故障处理：在系统发生故障时（如服务不可用、页面卡顿、服务调用异常等）需及时响应，优先通过应用层配置调整恢复业务；通过日志分析、链路追踪等手段定位根因，并要输出故障分析报告，故障排除后需要进行复盘，并提出相应的改进措施纳入应急预案；建立常见故障知识库，降低同类问题复发概率。

4.3.2.1.2.6.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.2.7业务能力中心(审批监管能力中心、调查监测能力中心、评价评估能力中心、预测预繁能力中心)

4.3.2.1.2.7.1服务内容

对审批监管能力中心、调查监测能力中心、评价评估能力中心、预测预防能力中心等模块提供运维服务，服务内容包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.2.7.1.1日常维护

对系统提供日常维护服务，主要包括资源管理、权限管理、版本发布管理、功能配置等，建立服务器、存储等资源的全生命周期动态台账，实现负载监控与扩缩容支持的闭环；基于实施账号权限最小化原则，对系统账号权限进行全流程管理，同时，开展账号日志审计与异常权限调整处理工作；遵循非高峰发布、预测试验证、灰度升级（单节点/集群滚动）灰度升级（单节点/集群滚动）等，确保版本迭代工作规范进行；同时提供系统功能配置优化服务，提升系统的业务适配性；形成“资源可溯、权限可控、发布可靠、配置高效”的日常维护模式，确保快速响应，保障系统稳定运行。日常维护主要工作内容如下：

4.3.2.1.2.7.1.1.1资源管理

梳理各类业务信息，记录业务资源的状态、进度、关联关系等关键信息。定期检查业务资源的使用情况，及时发现并处理资源冲突和异常。根据业务需求，对业务资源进行合理分配和调度，提高协同工作的效率。

4.3.2.1.2.7.1.1.2权限管理

提供权限管理服务，遵循最小权限原则与安全审计要求，集中管理运维相关账号，管控运维人员访问权限，仅允许授权人员通过可信网络接入；定期复核权限分配策略，调整权限、处理闲置账号，确保与安全管理要求一致；记录留存运维过程中的会话日志，支持事后追溯与合规审查。每月审查账号权限，确保符合最小权限原则和安全政策；审查操作系统关键角色权限、中间件权限、非结构化存储权限等，定期更新账号密码，保障系统及数据安全。系统变更或业务需求变化时，及时调整基础软件角色权限，保证时效性和准确性，支撑运维工作。低权限用户联调或排错需提权时，进行临时赋权，操作完成后及时回收权限，遵循最小权限原则。根据用户状态更新或回收账号，如账号所有者离场时回收其权限。

对应用账号建立覆盖全生命周期管理体系，包括账号的规范化创建、权限动态调整、离职/转岗账号冻结或注销等流程。按角色、业务场景精细化授权，确保权限最小化原则，避免越权访问。需定期开展账号权限审计，核查冗余账号、异常权限分配（如超管权限滥用），针对临时账号（如等保测评、密评等）需建立审批流程与时限控制机制，防范权限泄漏风险。

4.3.2.1.2.7.1.1.3系统版本发布

提供系统版本发布服务，当应用程序版本需要更新时，需要对新版本的软件系统发布进行规划，且需完成相关测试，验证新版本软件系统能够正常运行，才能进行正式的发布。若验证不通过，需要将新版本回退到原有版本。主要流程如下：

1、发布版本规划：确定发布计划，包括日期、内容、范围、方式、流程步骤、任务、责任人及时间节点等；确定发布时间，综合考量业务需求等因素，选在业务低峰期；制定备份策略，对系统文件、配置文件、数据库进行全量备份。

2、发布版本申请：按变更管理规范流程申请变更，审核人审核版本变更目标、时间计划、影响范围、风险评估及应对措施。

3、执行版本发布：单节点升级时，停止服务、执行升级、更新配置文件、启动服务并验证状态；集群滚动升级分批进行，通过负载均衡器路由流量；分布式系统升级分阶段进行，避免服务中断；功能验证时测试验证系统核心功能，检查日志及监控指标。发布测试验证不通过时，停止新版本服务，从备份恢复旧版本及配置文件，记录回滚原因及操作步骤，生成回滚报告。

4、系统更新后全链路验证：针对版本升级或配置调整，模拟真实用户操作路径，覆盖核心业务流程，验证功能完整性与业务连续性；开展高并发、异常场景压力测试，确保系统稳定性与容错能力。

5、持续监控与效果闭环：优化后通过AB测试、用户回访验证效果，确保版本发布后问题解决率达标。建立用户体验指标体系（操作成功

率、响应时间），长效跟踪系统使用情况。

4.3.2.1.2.7.1.1.4日常功能配置

提供日常功能配置服务，包括但不限于流程节点规则调整、表单字段增删、审批层级变更、系统进程配置优化等。针对高频配置场景，需提供模板化配置工具，提升效率并降低人工操作风险。所有配置操作需留存完整日志，支持事后追溯审计。

4.3.2.1.2.7.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：基于服务器、容器等基础资源及核心业务功能（如接口成功率、响应时间）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

4.3.2.1.2.7.1.2.1业务监控

提供业务功能监控服务，针对核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

4.3.2.1.2.7.1.2.2业务巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，如能力共享管理、指标管理等，页面响应时间>1000ms告警。

4.3.2.1.2.7.1.3技术支持

对系统提供技术支持服务，主要包括以下内容：通过标准化变更流程（需求评估、灰度发布、回滚验证）与配置管理数据库动态维护，保障系统变更可追溯、风险可控；围绕安全漏洞修复（版本升级、基线加固、弱密码整改）等保测评合规改造，提升系统抗风险能力；针对性能瓶颈开展架构调优（容器资源弹性扩缩、微服务链路治理），结合全链路压测验证效能提升；建立应急重保专班，按预案执行故障隔离、资源调配及快速恢复，完善“演练—处置—复盘”闭环；同步支撑功能配置动态调整、数据完整性维护及用户问题实时响应，形成“事前预防—事中控制—事后优化”的一体化响应体系，确保系统稳定性、安全性与业务连续性高效协同。具体服务内容如下：

4.3.2.1.2.7.1.3.1变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、数据增删改、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求提请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

（2）变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。

（3）变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。

（4）变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

4.3.2.1.2.7.1.3.2配置管理

提供配置管理服务，规范整个系统的配置管理流程。建立和维护标准化、系统化的配置管理台账，确保所有配置项都得到记录和控制。配置管理的服务内容如下：

(1) 配置关系梳理：确认配置范围、定义和标识配置项，梳理关联关系，制定配置管理机制、变更与审核流程机制、文档管理机制，形成体系化配置管理数据库。

(2) 配置数据录入：明确配置管理数据库所需配置信息和清单，录入配置项信息，确保准确性、适用性和可维护性。

(3) 配置数据更新：根据系统版本发布和变更情况，发起配置任务，更新配置库环境和调整配置基线；建立定期审查计划，排查与实际情况不匹配的情况；定期备份配置库，防止数据丢失。

4.3.2.1.2.7.1.3.3系统安全管理

提供系统安全管理服务，规范系统安全风险从接收、整改到验证的整个流程，具体服务内容如下：

(1) 安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。

(2) 安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。

(3) 安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。

(4) 整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。

(5) 整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改问题报告。

4.3.2.1.2.7.1.3.4应急与重保统筹组织

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

(1) 应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。

(2) 应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。

(3) 应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。

(4) 应急与重保支持：定期组织应急演练，模拟不同应急场景，验证预案可行性和团队协作效率，记录演练薄弱环节以便优化。

(5) 应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

4.3.2.1.2.7.1.3.5系统优化

提供系统优化服务，主要涉及对应用程序进行代码级别的优化、数据库查询效率的提升、用户界面的改进以及功能的适应性增强等方面。通过这两部分的优化，可以显著提高系统的整体性能，确保用户能够获得更加流畅和高效的使用体验。

提供应用架构与性能优化服务，对系统在高并发、大数据量场景下的性能瓶颈（如接口超时、数据库慢查询），提出应用优化方案，包括但不限于缓存策略调整、SQL优化、异步任务拆分、连接池调整等。确保关键应用服务响应时间符合业务要求，优化后需提供基准测试结果对比，量化性能提升效果。

首先，调研系统实际运行场景，梳理高并发、大数据量业务环节，明确性能评估重点。搭建贴近生产环境的测试环境，模拟实际业务流量，对系统进行压力测试与性能基准测试，精准定位性能瓶颈。借助专业性能分析工具，对系统运行数据进行全方位剖析，涵盖服务器资源使用情况、数据库查询日志、接口调用链路等，深入挖掘性能瓶颈根源。

基于性能评估结果，结合系统业务特点和未来发展规划，制定针对性的架构优化方案，包括但不限于异步任务重构、微服务架构适配等。制定详细计划，逐步推进架构与代码优化，确保业务不受影响；遵循规范与版本控制，严格审查与测试代码；优化后进行压力与基准测试，对比性能指标，验证方案有效性。根据性能验证结果，编制详细的基准测试对比报告，以数据与图表展示性能提升，如响应时间缩短、查询效率提高、吞吐量增加。对性能提升效果进行深入分析，阐述优化方案对政务软件系统的实际影响，提供客观、准确的性能评估依据。

4.3.2.1.2.7.1.3.6安全加固

提供业务应用加固服务，侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固；如越权访问、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

4.3.2.1.2.7.1.3.7备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日志分析及时提供技术支持，确保备份策略正常运行。

4.3.2.1.2.7.1.3.8演练与处置

配合提供定期应急演练与处置服务，模拟基础环境故障、业务异常宕机、数据误删、高可用切换等场景，检验应急预案有效性，演练后需填写应急手册包括故障切换步骤、联络清单等。

4.3.2.1.2.7.1.3.9业务支持

面向系统用户提供业务支持，提升用户在使用软件系统推进业务时的体验，在遇到疑问时能够及时获得相应的指引与建议。

4.3.2.1.2.7.1.4故障处理

对系统提供故障处理服务，以快速响应、精准定位、闭环管理为核心，构建覆盖“接收—分级—处置—验证—复盘”的规范化故障处理机制：通过监控告警、用户上报等多渠道接收故障，按业务影响分级响应，分派至对应团队紧急处置（如操作系统内核修复、数据库一致性恢复、中间件配置调优、网络拓扑排查及应用层服务重启等），结合日志分析、链路追踪定位根因，实施代码修复、环境回滚或资源扩容等方案；处置后通过全链路验证（功能、性能、数据一致性）确认恢复，释放临时资源并标准化配置；同步启动问题管理，对未根治故障及潜在缺陷进行根因分析，形成《问题报告》并沉淀至知识库，优化应急预案与监控策略；针对应用BUG，严格遵循“环境复现—测试验证—灰度发布”流程，确保修复代码安全上线，最终通过跨团队协作与经验复用，实现故障响应时效、修复质量及系统健壮性的三重提升，降低同类问题复发风险。故障处理工作主要包括以下具体工作内容：

4.3.2.1.2.7.1.4.1故障管理

整合故障反馈渠道，安排专人通过监控告警、巡检识别或用户上报等渠道发现接收故障需求，记录故障情况。一是初步识别故障，判断类型和影响范围，按业务重要性和影响范围划分故障等级和处置优先级。二是根据故障级别和类型，分派任务至对应运维人员处理，依据机制向相关人员通报故障情况和进度，记录时间节点。三是深入分析故障，制定处置方案，经领导同意后按职责实施处置。四是故障处理结束后，验证处理结果，检查系统运行情况和关键指标是否恢复正常，若未根本解决则记录信息和意见，触发问题解决与管理及变更管理流程。五是若处理过程中涉及临时增加资源的，需在完成故障处理闭环后，删除临时文件，释放系统资源，恢复配置或策略至标准状态，避免二次故障。故障修复一周内，总结故障经验形成报告，对重大故障启动复盘会议，优化应急预案和监控策略。

4.3.2.1.2.7.1.4.2问题管理

收集问题途径包括未根本解决的故障、日常巡检与监控告警、日志分析等，详细记录问题情况。判断问题类型与影响范围，组织技术专家联合进行根因分析，明确是否为已知错误或新发缺陷，提出处置与改进建议。根据建议制定处理计划，验证可行性后严格执行，防止故障再次发生和引入二次风险。问题发起方验证处理结果，确认解决且无副作用，比对运维基线数据，记录验证结果于《问题报告》。复盘分析问题根本原因

因，探讨从运维管理、系统架构设计、技术选型等方面优化，避免类似问题再次发生，沉淀为运维知识库案例。关闭前核对处理记录、验证结果及相关文档完整性，经双方签字确认；涉及配置修改或软件升级时，需变更管理流程审批，实施后回归测试确保未复发。

4.3.2.1.2.7.1.4.3应用缺陷修复

依据缺陷描述搭建与生产环境高度一致的测试环境，依照操作步骤执行复现，详细记录操作及系统响应，形成复现报告。运用工具和日志分析，结合复现报告定位代码错误位置和逻辑错误，深入剖析原因及对其他模块的影响。按修复方案进行代码修改，开展单元测试、集成测试、系统测试，验证修复后代码的正确性、集成情况及系统稳定性可靠性。制定发布计划，对修复代码打包部署前检查，按计划在生产环境发布，发布过程中监控系统运行状态，发布后验证并收集用户反馈。

4.3.2.1.2.7.1.4.4应用故障处理

应用故障处理：在系统发生故障时（如服务不可用、页面卡顿、服务调用异常等）需及时响应，优先通过应用层配置调整恢复业务；通过日志分析、链路追踪等手段定位根因，并要输出故障分析报告，故障排除后需要进行复盘，并提出相应的改进措施纳入应急预案；建立常见故障知识库，降低同类问题复发概率。

4.3.2.1.2.7.2服务成果

- 系统月度巡检报告；
- 系统月度变更报告；
- 系统故障处理报告（按需提供）；
- 系统年度运维服务总结报告。

4.3.2.1.2.8广东省自然资源一体化管理与服务平台（国土空间基础信息平台）-云GIS模块运维服务

4.3.2.1.2.8.1服务内容

4.3.2.1.2.8.1.1使用答疑

运维团队需具备专业的GIS知识和平台技术栈能力，能够快速诊断和解决GIS特有的问题（如地图服务异常、空间分析性能问题等）。对于用户在使用云GIS模块过程中遇到的问题提供技术支持及答疑服务，指导用户通过云GIS模块完成地图配置、服务配置、功能配置、服务优化等工作。

4.3.2.1.2.8.1.2日常运维

- 包括云GIS模块例行检查、定时任务管理、资源利用率监控、日志监控等，并根据运维情况提出优化方案，保障系统的正常运行。
- 实施7x24小时全方位监控，覆盖基础设施（CPU、内存、磁盘、网络）、云服务状态、GIS应用性能（服务响应时间、并发处理能力）、关键业务进程、日志异常和安全事件。要求设置合理的阈值，并能在异常发生或即将达到阈值时，通过多种渠道（短信、邮件、电话等）向指定人员主动、及时发出告警。

维护详尽、实时更新的相关运维文档，包括但不限于：系统架构图、部署手册、配置清单、操作手册、应急预案、故障处理知识库、变更记录。定期向用户提供运维报告（性能、事件、安全、变更）。在服务交接或关键变更时，进行必要的知识转移和培训。

4.3.2.1.2.8.1.3故障处理与问题解决

故障处理与问题解决：建立清晰的服务请求和事件处理流程，定义不同优先级（如P1-P4）的响应时间和解决时限。对于影响核心业务的高优先级故障（如服务中断、数据访问失败），要求在极短时间内（如15分钟）响应并启动应急处理流程。提供根本原因分析及解决报告。

4.3.2.1.2.8.1.4版本管理与升级优化

- 1.跟踪云GIS模块软件的版本更新和安全补丁，进行版本升级和补丁安装，保障升级后的云GIS模块与已有应用业务系统平滑对接，根据用户业务需求，开展云GIS模块功能升级服务。根据业务增长趋势和性能监控数据，进行科学的容量规划，提前预测资源需求（计算、存储、网络），并确保在业务高峰前完成资源弹性扩容，保障用户体验。定期进行安全审计、渗透测试和漏洞扫描。
- 2.云GIS地图打印服务接口的优化和升级完善。

4.3.2.1.2.8.2服务成果

- 系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告；

其他相关运维文档。

4.3.2.1.3广东省自然资源和不动产登记综合应用运行维护服务

广东省自然资源和不动产登记综合应用分别面向省级用户、市县级用户和公众企业用户三个领域提供共计18个模块，按业务系统和服务要求开展维护服务，包括自然资源和不动产登记综合应用门户、区块链+不动产登记模块、政务服务网不动产登记专题模块、不动产登记数据协同治理模块、不动产登记信息监管分析模块、不动产登记数据管理模块、不动产登记业务支撑模块、不动产登记业务管理模块、地籍管理模块、不动产登记资料管理模块、自然资源确权登记模块、不动产权属核查模块、自然资源权属争议调处信息管理模块、不动产登记信用管理模块、粤省事不动产登记专题模块、粤商通不动产登记专题模块、粤智助不动产登记专题模块、粤政易不动产登记交流服务模块。

运维内容主要包括：日常维护、例行巡检、技术支持和故障处理等，进一步保障业务连续性和服务质量。

4.3.2.1.3.1广东省不动产登记综合应用（省级端）

4.3.2.1.3.1.1服务内容

广东省不动产登记综合应用（省级端）包括：自然资源和不动产登记综合应用门户、不动产登记信息监管分析模块、不动产登记业务支撑模块、不动产登记数据协同治理模块、不动产登记数据管理模块、不动产权属核查模块、区块链+不动产登记模块和粤政易不动产登记交流服务模块。

运维内容包括日常运维、例行巡检、技术支持、故障处理等。

4.3.2.1.3.1.1.1日常运维

1、资源管理

梳理广东省自然资源和不动产登记综合应用（省级端）的各类业务信息，记录业务资源的状态、进度、关联关系等关键信息。定期检查业务资源的使用情况，及时发现并处理资源冲突和异常。根据业务需求，对业务资源进行合理分配和调度，提高协同工作的效率。

2、权限管理

建立广东省自然资源和不动产登记综合应用权限的规范化管理与维护体系，涵盖账号的规范化创建、权限的动态调整以及离职或转岗时账号的冻结或注销等流程。构建基于角色的访问控制（RBAC）模型，实现基于角色和业务场景的精细化授权，确保遵循权限最小化原则，防止越权访问。定期执行账号权限审计，审查冗余账号和异常权限分配（例如超管权限的滥用），并针对临时账号（如上线测评等保测评等）建立审批流程和时限控制机制，以防范权限泄露的风险。

（1）账号日常管理：构建全面覆盖应用账号生命周期的管理体系，包括账号从创建到注销的整个流程，涉及规范化创建、权限动态调整，以及在离职或转岗时对账号进行及时冻结或注销等操作。

（2）权限分级管理：根据角色和业务场景进行精细化授权，严格遵守权限最小化原则，以杜绝越权访问现象。

（3）账号权限定期审计：定期执行账号权限审计工作，重点审查冗余账号和异常权限分配问题，如超管权限的滥用，确保账号权限的合理性和合规性。

（4）临时账号管控：对临时账号实施严格管控，针对临时账号，建立审批流程并设定使用时限，有效预防因临时账号管理不当导致的权限泄漏风险。

3、日常监控

为了保证不动产登记信息监管分析模块、不动产登记业务支撑模块、不动产登记数据协同治理模块、不动产登记数据管理模块、不动产权属核查模块和区块链+不动产登记模块等核心业务模块的顺畅运行，开展业务应用的日常监控。监控机制覆盖了应用响应时间、接口成功率、并发连接数等多个重要指标，目的是对系统性能进行全面评估。另外，设立阈值告警机制，当监控指标超出预设的安全界限时，系统自动发出告警，以便运维人员能够迅速响应，实时跟踪系统运行状态，捕捉业务异常波动，通过日志分析及定位问题源头，并对异常情况进行调整，保障业务应用的稳定运行。

4、业务应用架构与性能优化

对自然资源与不动产登记综合应用（省级端）在高并发、大数据量场景下的性能瓶颈（如接口超时、数据库慢查询），提出架构优化方案，

包括但不限于缓存策略调整、慢SQL优化、异步任务拆分、资源动态分配调优等。确保关键应用服务响应时间符合业务要求，优化后需提供基准测试对比报告，量化性能提升效果。具体内容包

（1）现状评估与瓶颈诊断：分析实际运行场景，梳理高并发、大数据量业务环节，明确性能评估重点；搭建贴近生产环境的测试环境，模拟实际业务流量，对系统进行压力测试与性能基准测试，精准定位性能瓶颈；借助性能分析工具，对系统运行数据进行全方位剖析，涵盖服务器资源使用情况、数据库查询日志、接口调用链路等，深入挖掘性能瓶颈根源。

（2）设计架构优化方案：基于性能评估结果，结合业务特点和未来发展规划，制定针对性的架构优化方案，包括但不限于以下方面：

- 1）缓存策略优化：依据数据访问特性，通过优化缓存架构，提升数据读取速度，减轻数据库压力。
- 2）SQL 深度优化：针对数据库慢查询，全面优化 SQL 语句，合理设计表结构，规范数据存储，降低冗余，提高查询效率。
- 3）异步任务重构：将政务业务中的耗时任务拆分为异步任务，借助消息队列调度处理，避免阻塞主流程，增强系统并发与响应能力。
- 4）容器资源动态分配调优：通过合理配置资源请求与限制，结合水平自动扩缩容和垂直自动扩缩容，实现应用容器资源利用率与性能的平衡。借助集群自动扩缩容，优化节点资源分配，并通过服务分级策略保障核心业务优先级。利用监控工具提供实时数据监控，最终使得资源利用率提升，提升系统灵活性与可维护性。

（2）方案实施与验证：制定详细计划，明确任务、时间与责任人，逐步推进架构与代码优化，确保业务不受影响。遵循规范与版本控制，严格审查与测试代码，保障质量与稳定性；优化后进行压力与基准测试，对比性能指标，验证方案有效性；根据性能验证结果，编制详细的基准测试对比报告，以数据与图表展示性能提升，如响应时间缩短、查询效率提高、吞吐量增加。对性能提升效果进行深入分析，阐述优化方案对业务应用的实际影响，提供客观、准确的性能评估依据。

4.3.2.1.3.1.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：基于服务器、数据库、容器等基础资源及核心业务功能（如接口成功率、响应时间）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

1、业务监控

提供业务功能监控服务，针对核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

2、业务巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，如能力共享管理、指标管理等，页面响应时间>1000ms告警。

4.3.2.1.3.1.1.3技术支持

本服务旨在为自然资源和不动产登记综合应用（省级端）提供全面的技术支持。主要服务内容涵盖：

1、系统维护支持

构建专门的问题收集与反馈机制，由专职人员负责集中审核和分类问题，并根据分类结果确定问题的优先处理顺序，从而提升后端支持团队解决问题的效率。对于需要跨系统协作的事项，确保能够迅速协调处理。

2、变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、数据增删改、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件

系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求提请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

（2）变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。

（3）变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。

（4）变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

3、系统安全管理

提供系统安全管理服务，规范系统安全风险从问题接收、整改到验证的整个流程，具体服务内容如下：

（1）安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。

（2）安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。

（3）安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。

（4）整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。

（5）整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改闭环报告。

4、应急和重保统筹管理

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

（1）应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。

（2）应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。

（3）应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。

（4）应急与重保支持：定期组织应急演练，模拟不同应急场景，验证预案可行性和团队协作效率，记录演练薄弱环节以便优化。

（5）应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

5、安全加固

提供业务安全加固服务侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固；如越权访问、SQL注入、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

1）安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、SQL注入、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

2）漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

3）安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

6、备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略

可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日志分析及时提供技术支持，确保备份策略正常运行。

7、应急演练与处置

配合提供定期应急演练与处置服务，模拟基础环境故障、业务异常宕机、数据误删、高可用切换等场景，检验应急预案有效性，演练后需填写应急手册包括故障切换步骤、联络清单等。

8、电话热线支持

开通全天候（7*24小时）值班响应电话，由技术支持工程师负责接听申告。

9、远程技术支持

对于无法通过电话指导解决的故障，经服务对象同意后，通过远程接入方式登录故障设备进行诊断，查明故障原因，并指导现场维护人员进行故障处理。同时，提供系统接口文档和使用手册，以便现场人员进行有效维护。

10、现场技术支持

对于地市问题电话和远程支持均无法解决的故障，提供现场技术支持服务。派遣技术支持工程师前往现场，分析故障原因，制定并执行故障解决方案，确保问题得到妥善处理。

问题收集与反馈：对于非紧急问题，服务对象可填写“问题记录表”提交给运维服务人员。运维人员将定期整理问题解决情况，并形成服务报告反馈给服务对象。

4.3.2.1.3.1.1.4故障处理

对系统功能缺陷如业务办理失败、数据上报失败、统计结果偏差、流程异常、安全缺陷等问题提供系统缺陷（BUG）修复服务，包括缺陷复现、代码分析、测试验证及生产环境发布验证，具体如下：

1、缺陷复现

依据用户反馈或测试报告的操作步骤在测试环境（预发布环境）执行复现，详细记录每一步操作及系统响应，形成复现报告，清晰界定缺陷表现形式与触发条件。

2、代码分析

运用代码调试工具和日志分析手段，结合复现报告，精准定位导致缺陷的代码位置和逻辑错误。深入分析代码错误产生的原因，如业务逻辑错误、数据边界处理不当、接口调用异常等，并评估该缺陷对系统其他功能模块可能产生的影响。

3、修复实施与测试验证

按照修复方案进行代码修改，遵循代码规范和版本控制流程，保证代码的可维护性与可追溯性。修改完后依次开展系统测试，模拟生产环境进行全面测试，验证系统在各种业务场景下的稳定性与可靠性。

4、生产环境发布验证

制定详细的发布计划，明确发布时间、发布步骤、回滚方案等，对修复后的代码进行打包和部署前的最终检查，确保发布准备充分；然后按照发布计划，在生产环境进行代码发布。发布过程中密切监控系统运行状态，及时处理可能出现的问题；发布完成后，对系统进行全面验证，确保缺陷已完全修复，系统功能恢复正常。收集用户反馈，评估修复效果，为后续优化提供依据。

4.3.2.1.3.1.2服务成果

- （1）广东省自然资源和不动产登记综合应用运维服务周报；
- （2）广东省自然资源和不动产登记综合应用运维巡检月报；
- （3）广东省自然资源和不动产登记综合应用整改报告（按需提供）；
- （4）广东省自然资源和不动产登记综合应用运维服务总结报告。

4.3.2.1.3.2广东省不动产登记综合应用（市县端）

4.3.2.1.3.2.1服务内容

广东省不动产登记综合应用（市县端）包括：不动产登记业务管理模块、地籍管理模块、不动产登记资料管理模块、自然资源确权登记模块、自然资源权属争议调处信息管理模块和不动产登记信用管理模块。

运维内容包括日常运维、例行巡检、技术支持、故障处理等。

4.3.2.1.3.2.1.1日常运维

1、资源管理

梳理广东省自然资源和不动产登记综合应用（市县端）的各类业务信息，记录业务资源的状态、进度、关联关系等关键信息。定期检查业务资源的使用情况，及时发现并处理资源冲突和异常。根据业务需求，对业务资源进行合理分配和调度，提高协同工作的效率。

2、权限管理

建立广东省自然资源和不动产登记综合应用权限的规范化管理与维护体系，涵盖账号的规范化创建、权限的动态调整以及离职或转岗时账号的冻结或注销等流程。构建基于角色的访问控制（RBAC）模型，实现基于角色和业务场景的精细化授权，确保遵循权限最小化原则，防止越权访问。定期执行账号权限审计，审查冗余账号和异常权限分配（例如超管权限的滥用），并针对临时账号（如上线测评等保测评等）建立审批流程和时限控制机制，以防范权限泄露的风险。

（1）账号日常管理：构建全面覆盖应用账号生命周期的管理体系，包括账号从创建到注销的整个流程，涉及规范化创建、权限动态调整，以及在离职或转岗时对账号进行及时冻结或注销等操作。

（2）权限分级管理：根据角色和业务场景进行精细化授权，严格遵守权限最小化原则，以杜绝越权访问现象。

（3）账号权限定期审计：定期执行账号权限审计工作，重点审查冗余账号和异常权限分配问题，如超管权限的滥用，确保账号权限的合理性和合规性。

（4）临时账号管控：对临时账号实施严格管控，针对临时账号，建立审批流程并设定使用时限，有效预防因临时账号管理不当导致的权限泄漏风险。

3、日常监控

为了保证不动产登记业务管理模块、地籍管理模块、不动产登记资料管理模块、自然资源确权登记模块、自然资源权属争议调处信息管理模块和不动产登记信用管理模块等业务模块的顺畅运行，开展业务应用的日常监控。监控机制覆盖了应用响应时间、接口成功率、并发连接数等多个重要指标，目的是对系统性能进行全面评估。另外，设立阈值告警机制，当监控指标超出预设的安全界限时，系统自动发出告警，以便运维人员能够迅速响应，实时跟踪系统运行状态，捕捉业务异常波动，通过日志分析及及时定位问题源头，并对异常情况进行调整，保障业务应用的稳定运行。

4、业务应用配置维护

为广东省自然资源和不动产登记综合应用（市县端）提供业务配置运维服务，并对配置操作均记录版本与日志，以支持后续的追溯审计工作，具体服务内容包括：

（1）业务动态配置服务：为业务参数提供动态配置支持，内容涵盖流程节点规则的调整、表单字段的增删、审批层级的变更、系统进程配置的优化等多方面配置需求。

（2）操作日志留存服务：系统将记录历史配置历史版本与操作的日志，为后续的追溯与审计工作提供有力的证据支持。

5、业务应用数据维护

为广东省自然资源和不动产登记综合应用（市县端）中的6个子模块所使用的数据信息提供存储、交换、导出、备份恢复、处理维护等维护服务，确保各类数据管理等方面的高效性和安全性。主要包括：

（1）数据存储服务：包括数据版本的维护、数据占用空间的维护、数据存储位置的维护、数据分级存储的维护以及数据存储系统的维护等服务内容，从而确保数据的完整性和可访问性，同时优化存储资源的使用效率。

（2）数据交换服务：主要对广东省自然资源和不动产登记综合应用与其他业务应用间、应用内部上下级部门间以及不同政府机关间的数据进行交换管理，确保信息在各个系统和部门之间顺畅流通，提高工作效率，同时保障信息交换的安全性和准确性。

（3）数据导出服务：根据用户根据需要导出特定范围内的数据，灵活提供数据导出服务，方便用户获取所需信息。

（4）数据备份与恢复：依托云平台、人大金仓数据库的备份与恢复能力，制定完整的数据备份方案并提供备份服务，当应用更新前保存历史数据，更新后及时备份新应用系统版本，以防在应用系统崩溃后能够快速的从备份数据中恢复过来，使系统能够在短时间内快速解决故障。

（5）数据处理维护：根据地市提交数据维护工单或厅主管部门管理要求，对数据进行管理和维护，包括但不限于数据的查询与分析，识别数据重复、数据错误、数据格式化不一致等问题并进行处理，以提高数据质量，以确保数据的完整性和可用性。

6、业务应用架构与性能优化

对自然资源与不动产登记综合应用（市县端）在高并发、大数据量场景下的性能瓶颈（如接口超时、数据库慢查询），提出架构优化方案，包括但不限于缓存策略调整、慢SQL优化、异步任务拆分、资源动态分配调优等。确保关键应用服务响应时间符合业务要求，优化后需提供基准测试对比报告，量化性能提升效果。具体内容包括：

（1）现状评估与瓶颈诊断：分析实际运行场景，梳理高并发、大数据量业务环节，明确性能评估重点；搭建贴近生产环境的测试环境，模拟实际业务流量，对系统进行压力测试与性能基准测试，精准定位性能瓶颈；借助性能分析工具，对系统运行数据进行全方位剖析，涵盖服务器资源使用情况、数据库查询日志、接口调用链路等，深入挖掘性能瓶颈根源。

（2）设计架构优化方案：基于性能评估结果，结合业务特点和未来发展规划，制定针对性的架构优化方案，包括但不限于以下方面：

1）缓存策略优化：依据数据访问特性，通过优化缓存架构，提升数据读取速度，减轻数据库压力。

2）SQL 深度优化：针对数据库慢查询，全面优化 SQL 语句，合理设计表结构，规范数据存储，降低冗余，提高查询效率。

3）异步任务重构：将政务业务中的耗时任务拆分为异步任务，借助消息队列调度处理，避免阻塞主流程，增强系统并发与响应能力。

4）容器资源动态分配调优：通过合理配置资源请求与限制，结合水平自动扩缩容和垂直自动扩缩容，实现应用容器资源利用率与性能的平衡。借助集群自动扩缩容，优化节点资源分配，并通过服务分级策略保障核心业务优先级。利用监控工具提供实时数据监控，最终使得资源利用率提升，提升系统灵活性与可维护性。

（2）方案实施与验证：制定详细计划，明确任务、时间与责任人，逐步推进架构与代码优化，确保业务不受影响。遵循规范与版本控制，严格审查与测试代码，保障质量与稳定性；优化后进行压力与基准测试，对比性能指标，验证方案有效性；根据性能验证结果，编制详细的基准测试对比报告，以数据与图表展示性能提升，如响应时间缩短、查询效率提高、吞吐量增加。对性能提升效果进行深入分析，阐述优化方案对业务应用的实际影响，提供客观、准确的性能评估依据。

4.3.2.1.3.2.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：基于服务器、数据库、容器等基础资源及核心业务功能（如接口成功率、响应时间）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

1、业务监控

提供业务功能监控服务，针对核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

2、业务巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，如能力共享管理、指标管理等，页面响应时间>1000ms告警。

4.3.2.1.3.2.1.3技术支持

本服务旨在为自然资源和不动产登记综合应用（市县端）提供全面的技术支持。主要服务内容涵盖：

1、系统维护支持

构建专门的问题收集与反馈机制，由专职人员负责集中审核和分类问题，并根据分类结果确定问题的优先处理顺序，从而提升后端支持团队解决问题的效率。对于需要跨系统协作的事项，确保能够迅速协调处理。

2、变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、数据增删改、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求提请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

（2）变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。

（3）变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。

（4）变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

3、系统安全管理

提供系统安全管理服务，规范系统安全风险从问题接收、整改到验证的整个流程，具体服务内容如下：

（1）安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。

（2）安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。

（3）安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。

（4）整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。

（5）整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改闭环报告。

4、应急和重保统筹管理

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

（1）应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。

（2）应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。

（3）应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。

（4）应急与重保支持：定期组织应急演练，模拟不同应急场景，验证预案可行性和团队协作效率，记录演练薄弱环节以便优化。

（5）应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

5、安全加固

提供业务应用安全加固服务，侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固：如越权访问、SQL注入、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

1）安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、SQL注入、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

2）漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

3）安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

6、备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日志分析及时提供技术支持，确保备份策略正常运行。

7、应急演练与处置

配合提供定期应急演练与处置服务，模拟基础环境故障、业务异常宕机、数据误删、高可用切换等场景，检验应急预案有效性，演练后需填写应急手册包括故障切换步骤、联络清单等。

8、电话热线支持

开通全天候（7*24小时）值班响应电话，由技术支持工程师负责接听申告。

9、远程技术支持

对于无法通过电话指导解决的故障，经服务对象同意后，通过远程接入方式登录故障设备进行诊断，查明故障原因，并指导现场维护人员进行故障处理。同时，提供系统接口文档和使用手册，以便现场人员进行有效维护。

10、现场技术支持

对于地市问题电话和远程支持均无法解决的故障，提供现场技术支持服务。派遣技术支持工程师前往现场，分析故障原因，制定并执行故障解决方案，确保问题得到妥善处理。

问题收集与反馈：对于非紧急问题，服务对象可填写“问题记录表”提交给运维服务人员。运维人员将定期整理问题解决情况，并形成服务报告反馈给服务对象。

4.3.2.1.3.2.1.4故障处理

对系统功能缺陷如业务办理失败、数据上报失败、统计结果偏差、流程异常、安全缺陷等问题提供系统缺陷（BUG）修复服务，包括缺陷复现、代码分析、测试验证及生产环境发布验证，具体如下：

1、缺陷复现

依据用户反馈或测试报告的操作步骤在测试环境（预发布环境）执行复现，详细记录每一步操作及系统响应，形成复现报告，清晰界定缺陷表现形式与触发条件。

2、代码分析

运用代码调试工具和日志分析手段，结合复现报告，精准定位导致缺陷的代码位置和逻辑错误。深入分析代码错误产生的原因，如业务逻辑错误、数据边界处理不当、接口调用异常等，并评估该缺陷对系统其他功能模块可能产生的影响。

3、修复实施与测试验证

按照修复方案进行代码修改，遵循代码规范和版本控制流程，保证代码的可维护性与可追溯性。修改完后依次开展系统测试，模拟生产环境进行全面测试，验证系统在各种业务场景下的稳定性与可靠性。

4、生产环境发布验证

制定详细的发布计划，明确发布时间、发布步骤、回滚方案等，对修复后的代码进行打包和部署前的最终检查，确保发布准备充分；然后按照发布计划，在生产环境进行代码发布。发布过程中密切监控系统运行状态，及时处理可能出现的问题；发布完成后，对系统进行全面验证，确保缺陷已完全修复，系统功能恢复正常。收集用户反馈，评估修复效果，为后续优化提供依据。

4.3.2.1.3.2.2服务成果

- （1）广东省自然资源和不动产登记综合应用运维服务周报；
- （2）广东省自然资源和不动产登记综合应用运维巡检月报；
- （3）广东省自然资源和不动产登记综合应用整改报告（按需提供）；
- （4）广东省自然资源和不动产登记综合应用运维服务总结报告。

4.3.2.1.3.3广东省不动产登记综合应用（公众侧）

4.3.2.1.3.3.1服务内容

广东省不动产登记综合应用（公众侧）包括：政务服务网不动产登记专题模块、粤省事不动产登记专题模块、粤商通不动产登记专题模块和粤智助不动产登记专题模块。

运维内容包括日常运维、例行巡检、技术支持、故障处理等。

4.3.2.1.3.3.1.1日常运维

1、资源管理

梳理广东省自然资源和不动产登记综合应用（市县端）的各类业务信息，记录业务资源的状态、进度、关联关系等关键信息。定期检查业务资源的使用情况，及时发现并处理资源冲突和异常。根据业务需求，对业务资源进行合理分配和调度，提高协同工作的效率。

2、日常监控

为了保证政务服务网不动产登记专题模块、粤省事不动产登记专题模块、粤商通不动产登记专题模块和粤智助不动产登记专题模块等业务模块的顺畅运行，开展业务应用的日常监控。监控机制覆盖了应用响应时间、接口成功率、并发连接数等多个重要指标，目的是对系统性能进行全面评估。另外，设立阈值告警机制，当监控指标超出预设的安全界限时，系统自动发出告警，以便运维人员能够迅速响应，实时跟踪系统运行状态，捕捉业务异常波动，通过日志分析及及时定位问题源头，并对异常情况进行调整，保障业务应用的稳定运行。

4.3.2.1.3.3.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：基于服务器、数据库、容器等基础资源及核心业务功能（如接口成功率、响应时间）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

1、业务监控

提供业务功能监控服务，针对核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

2、业务巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，如能力共享管理、指标管理等，页面响应时间>1000ms告警。

4.3.2.1.3.3.1.3技术支持

本服务旨在为自然资源和不动产登记综合应用（公众侧）提供全面的技术支持。主要服务内容涵盖：

1、系统维护支持

构建专门的问题收集与反馈机制，由专职人员负责集中审核和分类问题，并根据分类结果确定问题的优先处理顺序，从而提升后端支持团队解决问题的效率。对于需要跨系统协作的事项，确保能够迅速协调处理。

2、变更管理

提供变更管理服务，规范系统的日常变更操作，保障系统功能稳定运行；当系统涉及服务功能迭代、停机维护、数据增删改、资源调整、架构优化、备份恢复等操作时，为降低人为误操作风险，需建立覆盖变更全生命周期的管理制度。通过标准化审批、风险评估及回滚机制，对软件系统变更全流程进行统一管理，确保变更可追溯、可控制，保障系统稳定性与业务连续性。主要变更管理流程包括：

（1）变更提出与接收：根据需求提请对信息系统进行变更操作，说明变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤及回退步骤，运维人员记录变更需求。

- (2) 变更评估与审核：评估变更操作的必要性和可行性，分析影响范围和风险，对变更操作进行审核。
- (3) 变更实施：变更请求通过审核后，告知受影响的上下游系统和用户，运维人员执行变更操作，并监管进度跟踪实施过程。
- (4) 变更确认和回顾：对变更结果进行确认，评估是否满足需求，决策是否回退，回顾总结变更过程，编写变更报告。

3、系统安全管理

提供系统安全管理服务，规范系统安全风险从问题接收、整改到验证的整个流程，具体服务内容如下：

- (1) 安全通报接收：接收云平台等保测评等安全服务方的安全通报，详细记录通报来源、时间、风险内容、等级、影响范围等关键内容。
- (2) 安全问题分类：按技术维度和业务维度对接收的安全问题进行分类，判断处置优先级，指导整改资源分配。
- (3) 安全整改任务分派：根据分类结果，分派整改任务至责任人，明确整改措施、时限及回滚方案。
- (4) 整改执行与监控：在测试环境验证整改方案，灰度发布至生产环境，实时监控整改效果，确保无业务异常，记录完整操作日志。
- (5) 整改情况报告：汇总整改结果、剩余风险及改进建议，形成安全整改闭环报告。

4、应急和重保统筹管理

提供应急与重保统筹组织服务，为自然资源厅重要系统提供应急响应和重要时点保障，设立应急重保工作组，应急重保工作组主要由一、二、三线和其他运维支撑人员组成，主要负责应急预案和重保方案的编制、应急响应处置、应急与重保支持、应急与重保总结等工作。主要应急与重保统筹组织流程包括：

- (1) 应急重保工作组组建：根据技术能力需求和保障工作要求，抽调技术、运维、安全等领域人员成立工作组，明确岗位和责任分工，确保具备快速响应和协同处置能力。
- (2) 应急预案与重保方案编制：结合系统特点和历史风险数据，制定详细应急预案和重保方案。应急预案设计不同场景应急流程，明确处置步骤、资源调配、恢复策略等；重保方案针对重大活动或特殊时期制定值班安排、汇报机制、故障通报通报机制等。
- (3) 应急响应处置：应急事件发生后，启动应急响应流程，按预案和方案执行响应处置，快速定位问题、隔离故障、调配资源修复，通报通报至相关人员与领导，记录事件全过程。
- (4) 应急与重保支持：定期组织应急演练，模拟不同应急场景，验证预案可行性和团队协作效率，记录演练薄弱环节以便优化。
- (5) 应急与重保总结：完成应急处置和重保工作后，回顾总结全流程，输出处置总结报告，支撑日后应急响应工作优化完善。

5、安全加固

提供业务应用安全加固服务，侧重于保护应用程序免受攻击，这包括代码审计、漏洞扫描和定期的安全测试等，此外，还需要确保应用数据传输过程中的加密，以及对敏感数据进行适当的保护措施。

针对云安全监控等保测评或密评反馈的应用安全问题进行修复加固；如越权访问、SQL注入、敏感信息泄露、未授权访问等风险。通过提供加固方案并修复系统漏洞，保证系统安全。修复漏洞前需要进行充分的测试验证，避免影响正常业务开展。

1) 安全风险识别与方案制定：综合云安全监控告警日志等保测评报告、密评反馈结果等，完整梳理政务软件系统面临的应用安全风险，包括但不限于越权访问、SQL注入、敏感信息泄露、未授权访问等。依据系统的重要性、数据敏感程度以及风险影响范围，对识别出的安全风险进行等级划分，明确重点防护对象与优先处理顺序。

针对不同类型安全风险，制定详细加固方案，确保方案符合政务领域相关安全法规、标准与规范要求，保障系统合规运行。

2) 漏洞修复与加固实施：搭建仿真测试环境，对加固方案进行全面测试，确保加固措施不影响系统正常运行。依据风险等级与业务影响，分阶段推进漏洞修复与加固，优先处理高风险漏洞，确保核心功能与数据安全，并实时监控系统状态，及时处理问题。

3) 安全加固效果评估：制定涵盖安全风险消除、漏洞修复率、防护能力提升的评估指标体系；加固后进行全面安全评估，验证措施有效性，并编制详细报告，为政务部门提供决策依据。

6、备份管理与恢复

根据软件系统备份需求，提供备份管理与恢复服务；对软件系统关键的配置信息和重要数据进行梳理，明确备份的路径信息；然后，根据业务连续性、运行情况及数据安全等级要求制定备份对象的备份策略和恢复策略，明确备份任务执行时间、执行频率、保存期限等，评估备份策略可用性。备份策略下发后，选择对应的备份方案，协助完成备份工具的接入和调试。定期查看备份作业执行状态，关注失败或报错情况，根据日志分析及时提供技术支持，确保备份策略正常运行。

7、应急演练与处置

配合提供定期应急演练与处置服务，模拟基础环境故障、业务异常宕机、数据误删、高可用切换等场景，检验应急预案有效性，演练后需填写应急手册包括故障切换步骤、联络清单等。

8、电话热线支持

开通全天候（7*24小时）值班响应电话，由技术支持工程师负责接听申告。

9、远程技术支持

对于无法通过电话指导解决的故障，经服务对象同意后，通过远程接入方式登录故障设备进行诊断，查明故障原因，并指导现场维护人员进行故障处理。同时，提供系统接口文档和使用手册，以便现场人员进行有效维护。

10、现场技术支持

对于地市问题电话和远程支持均无法解决的故障，提供现场技术支持服务。派遣技术支持工程师前往现场，分析故障原因，制定并执行故障解决方案，确保问题得到妥善处理。

问题收集与反馈：对于非紧急问题，服务对象可填写“问题记录表”提交给运维服务人员。运维人员将定期整理问题解决情况，并形成服务报告反馈给服务对象。

4.3.2.1.3.3.1.4故障处理

对系统功能缺陷如业务办理失败、数据上报失败、统计结果偏差、流程异常、安全缺陷等问题提供系统缺陷（BUG）修复服务，包括缺陷复现、代码分析、测试验证及生产环境发布验证，具体如下：

1、缺陷复现

依据用户反馈或测试报告的操作步骤在测试环境（预发布环境）执行复现，详细记录每一步操作及系统响应，形成复现报告，清晰界定缺陷表现形式与触发条件。

2、代码分析

运用代码调试工具和日志分析手段，结合复现报告，精准定位导致缺陷的代码位置和逻辑错误。深入分析代码错误产生的原因，如业务逻辑错误、数据边界处理不当、接口调用异常等，并评估该缺陷对系统其他功能模块可能产生的影响。

3、修复实施与测试验证

按照修复方案进行代码修改，遵循代码规范和版本控制流程，保证代码的可维护性与可追溯性。修改完后依次开展系统测试，模拟生产环境进行全面测试，验证系统在各种业务场景下的稳定性与可靠性。

4、生产环境发布验证

制定详细的发布计划，明确发布时间、发布步骤、回滚方案等，对修复后的代码进行打包和部署前的最终检查，确保发布准备充分；然后按照发布计划，在生产环境进行代码发布。发布过程中密切监控系统运行状态，及时处理可能出现的问题；发布完成后，对系统进行全面验证，确保缺陷已完全修复，系统功能恢复正常。收集用户反馈，评估修复效果，为后续优化提供依据。

4.3.2.1.3.3.2服务成果

- （1）广东省自然资源和不动产登记综合应用运维服务周报；
- （2）广东省自然资源和不动产登记综合应用运维巡检月报；
- （3）广东省自然资源和不动产登记综合应用整改报告（按需提供）；
- （4）广东省自然资源和不动产登记综合应用运维服务总结报告。

4.3.2.1.4广东省国土空间用途管制综合应用运行维护服务

4.3.2.1.4.1服务内容

业务系统运维内容为用途管制综合应用：用地审批管理、矿产资源审批管理、海域使用管理、重大项目全流程监管、项目策划生成、指标管理、项目库管理、图形审查、综合管理等模块日常维护、例行巡检、故障处理、业务保障、安全加固等。

4.3.2.1.4.1.1日常维护

1、系统运行监控

梳理广东省国土空间用途管制综合应用的各类业务信息，记录业务资源的状态、进度、关联关系等关键信息。定期检查业务资源的使用情

况，及时发现并处理资源冲突和异常。根据业务需求，对业务资源进行合理分配和调度，提高协同工作的效率。利用监控工具实时查看系统操作日志，监控是否有非法的数据删除、异常登录、登出操作等信息，及时发现并处理异常行为。定期查看系统日志、操作日志及系统相关的软硬件设备运行日志，判断是否有运行错误信息，定期备份日志，确保日志信息完整可追溯。

2、用户访问管理

建立广东省国土空间用途管制综合应用权限的规范化管理与维护体系，涵盖账号的规范化创建、权限的动态调整以及离职或转岗时账号的冻结或注销等流程。构建基于角色的访问控制（RBAC）模型，实现基于角色和业务场景的精细化授权，确保遵循权限最小化原则，防止越权访问。定期执行账号权限审计，审查冗余账号和异常权限分配（例如超管权限的滥用），并针对临时账号（如上线测评等保测评等）建立审批流程和时限控制机制，以防范权限泄露的风险。

（1）账号日常管理：构建全面覆盖应用账号生命周期的管理体系，包括账号从创建到注销的整个流程，涉及规范化创建、权限动态调整，以及在离职或转岗时对账号进行及时冻结或注销等操作。

（2）权限分级管理：根据角色和业务场景进行精细化授权，严格遵守权限最小化原则，以杜绝越权访问现象。

（3）账号权限定期审计：定期执行账号权限审计工作，重点审查冗余账号和异常权限分配问题，如超管权限的滥用，确保账号权限的合理性和合规性。

（4）临时账号管控：对临时账号实施严格管控，针对临时账号，建立审批流程并设定使用时限，有效预防因临时账号管理不当导致的权限泄漏风险。

（5）账号安全管理：定期开展与系统安全相关的弱口令、异常账号等问题排查与处理。

3、日常监控

为了保证广东省国土空间用途管制综合应用的顺畅运行，开展业务应用的日常监控。监控机制覆盖了应用响应时间、接口成功率、并发连接数、资源使用情况等多个重要指标，目的是对系统性能进行全面评估。另外，设立阈值告警机制，当系统及其正常运行依赖的资源相关监控指标超出预设的安全界限时（如响应时间长于要求的指标、接口成功率低于要求的指标、并发连接数少于要求的指标、资源低负载、资源超负荷等），系统自动发出告警，以便运维人员能够迅速响应，实时跟踪系统运行状态，捕捉业务异常波动，通过日志分析及时定位问题源头，并对异常情况进行调整，保障业务应用的稳定运行。

4、业务应用架构优化

对广东省国土空间用途管制综合应用在高并发、大数据量场景下的性能瓶颈（如接口超时、数据库慢查询），提出架构优化方案，包括但不限于缓存策略调整、慢SQL优化、异步任务拆分、资源动态分配调优等。确保关键应用服务响应时间符合业务要求，优化后需提供基准测试对比报告，量化性能提升效果。具体内容包括：

（1）现状评估与瓶颈诊断：分析实际运行场景，梳理高并发、大数据量业务环节，明确性能评估重点；搭建贴近生产环境的测试环境，模拟实际业务流量，对系统进行压力测试与性能基准测试，精准定位性能瓶颈；借助性能分析工具，对系统运行数据进行全方位剖析，涵盖服务器资源使用情况、数据库查询日志、接口调用链路等，深入挖掘性能瓶颈根源。

（2）设计架构优化方案：基于性能评估结果，结合业务特点和未来发展规划，制定针对性的架构优化方案，包括但不限于以下方面：

1）缓存策略优化：依据数据访问特性，通过优化缓存架构，提升数据读取速度，减轻数据库压力。

2）SQL 深度优化：针对数据库慢查询，全面优化 SQL 语句，合理设计表结构，规范数据存储，降低冗余，提高查询效率。

3）异步任务重构：将政务业务中的耗时任务拆分为异步任务，借助消息队列调度处理，避免阻塞主流程，增强系统并发与响应能力。

4）容器资源动态分配调优：通过合理配置资源请求与限制，结合水平自动扩缩容和垂直自动扩缩容，实现应用容器资源利用率与性能的平衡。借助集群自动扩缩容，优化节点资源分配，并通过服务分级策略保障核心业务优先级。利用监控工具提供实时数据监控，最终使得资源利用率提升，提升系统灵活性与可维护性。

（2）方案实施与验证：制定详细计划，明确任务、时间与责任人，逐步推进架构与代码优化，确保业务不受影响。遵循规范与版本控制，严格审查与测试代码，保障质量与稳定性；优化后进行压力与基准测试，对比性能指标，验证方案有效性；根据性能验证结果，编制详细的基准测试对比报告，以数据与图表展示性能提升，如响应时间缩短、查询效率提高、吞吐量增加。对性能提升效果进行深入分析，阐述优化方案对业务应用的实际影响，提供客观、准确的性能评估依据。

5.配置管理与维护

根据需要对广东省国土空间用途管制综合应用系统相关配置文件进行调整，包括但不限于由于软硬件环境升级、变更等引起的设备变化，系统安全漏洞修复引起的变化，系统扩展引起的变化等，同时对系统涉及的环境资源信息进行记录维护，管理系统涉及的软硬件设备、系统物理和逻辑关系，确保系统架构清晰、稳定。

4.3.2.1.4.1.2例行巡检

对系统提供例行巡检服务，通过实时监控、阈值告警、定期巡检三层协同联动机制，保障系统与业务稳定运行：基于服务器、数据库、容器等基础资源及核心业务功能（如接口成功率、响应时间、资源使用情况等）的实时指标采集与动态告警，实现异常秒级感知；结合每日定期巡检，及时发现系统隐患；通过周期性报告沉淀优化建议，推动监控基线、告警策略及巡检方案的持续优化，有效提升巡检效率，降低业务中断风险，提升系统可用性。例行巡检主要包括以下内容：

1、业务监控

提供业务功能监控服务，针对核心业务功能实施监控，涵盖应用响应时间、接口成功率、并发连接数等关键指标，构建阈值告警机制，确保异常时及时响应。每日开展人工与自动化相结合的巡检工作，重点排查数据库负载、告警信息、连接池状态、应用报错日志、接口调用异常信息等潜在隐患，保障业务应用稳定运行。制定例行巡检方案，定期对软件系统及其正常运行依赖的资源进行例行巡检。针对性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

2、业务巡检

提供业务功能巡检服务，设定业务应用巡检项，制定例行巡检方案，定期对软件系统进行例行巡检。针对软件系统及其正常运行依赖的资源性能指标、可用性等方面设定巡检项，合理安排巡检计划。争取在造成业务故障前，通过检查分析，提前发现系统的故障异常、软件告警、潜在问题、安全隐患等，并及时做出适当的处置，保障系统运行状况良好，防止故障发生，降低业务故障风险与负面影响，确保软件系统能够正常运行。

通过进程及日志，查看应用后台进程，查看程序进程是否存在；

通过页面拨测，检查功能模块，如能力共享管理、指标管理等，页面响应时间>1000ms告警。

4.3.2.1.4.1.3故障处理

对系统功能及其正常运行依赖的资源缺陷如业务办理失败、数据上报失败、统计结果偏差、流程异常、功能异常、安全缺陷等问题提供系统缺陷（BUG）修复服务，对由于人为因素、环境原因或者黑客攻击、病毒感染或恶意软件入侵等引发的系统异常、系统中断、系统瘫痪、数据篡改、数据丢失或数据泄露问题提供系统及软硬件和网络故障的处理修复服务。包括缺陷复现、代码分析、测试验证及生产环境发布验证，具体如下：

1、缺陷复现

依据用户反馈、测试报告、安全报告的操作步骤在测试环境（预发布环境）执行复现，详细记录每一步操作及系统响应，形成复现报告，清晰界定缺陷表现形式与触发条件。

2、代码分析

运用代码调试工具和日志分析手段，结合复现报告，精准定位导致缺陷的代码位置和逻辑错误。深入分析代码错误产生的原因，如业务逻辑错误、数据边界处理不当、接口调用异常等，并评估该缺陷对系统其他功能模块可能产生的影响。

3、修复实施与测试验证

按照修复方案进行代码修改，遵循代码规范和版本控制流程，保证代码的可维护性与可追溯性。修改完后依次开展系统测试，模拟生产环境进行全面测试，验证系统在各种业务场景下的稳定性与可靠性。

4、生产环境发布验证

制定详细的发布计划，明确发布时间、发布步骤、回滚方案等，对修复后的代码进行打包和部署前的最终检查，确保发布准备充分；然后按照发布计划，在生产环境进行代码发布。发布过程中密切监控系统运行状态，及时处理可能出现的问题；发布完成后，对系统进行全面验证，确保缺陷已完全修复，系统功能恢复正常。收集用户反馈，评估修复效果，为后续优化提供依据。

4.3.2.1.4.1.4业务保障

要求对系统提供业务保障服务。应用系统业务保障是业务正常办理的关键内容，也是制约系统应用及发展水平的关键因素，要求管理和维护

人员既要熟悉各类业务，又要熟悉相应应用系统的使用及维护，起到工程应用单位和系统开发单位之间的纽带作用。重点在以下几方面加强管理和维护，使系统能够高效而安全的运行：

1.业务流程优化

根据广东省国土空间用途管制综合应用系统的实际使用情况和用户反馈，对系统的业务流程进行优化调整，提高系统的易用性和工作效率。例如，优化审批流程、简化数据录入步骤、增加批量操作功能等，以满足用户不断变化的业务需求。

2.业务表单管理

建立对业务表单数据质量监控机制，定期对系统中的数据进行检查和清理，确保数据的准确性、完整性和一致性。

对于发现业务表单的数据质量问题，及时进行修复和更新，同时分析数据质量问题产生的原因，制定相应的数据质量改进措施，防止类似问题再次发生。

3.系统性能优化

根据系统的运行情况和用户需求，对系统的性能进行优化调整。例如，优化数据库查询语句、调整服务器资源配置、升级系统软件版本等，以提高系统的响应速度和并发处理能力，确保系统在高负载情况下能够稳定运行。

4.业务支持

支持业务科室对系统功能的日常使用，协助解决使用过程中遇到的问题。

支持客户端运行环境的日常维护，确保客户端能够正常访问系统。

跟踪判断提出的问题，与业务科室交流需求点，判断问题是否存在或使用不当。

将系统问题提交给支持环节，及时反馈问题处理进度，对领导负责。

提供系统功能使用支持，包括客户端程序更新使用支持、用户密码修改支持、机构人员角色权限配置调整等。

协助进行业务流程调整和修改、表单修改，确保业务流程顺畅。

对在办项目改派、结案项目变更、业务数据修改提供支持，保障业务数据准确。

提供打印机设置及报表打印支持，确保报表输出符合业务需求。

对无法办理的项目进行跟踪反馈，及时解决问题，保障业务正常开展。

4.3.2.1.4.1.5安全加固

根据安全检查、安全扫描、安全测评要求和用户需求，及时修复系统漏洞，升级、更新系统正常运行相关的资源，处理安全隐患，保证系统安全。具体涵盖如下几个方面：

1.系统漏洞扫描与修复

定期对广东省国土空间用途管制综合应用系统进行全面的安全漏洞扫描，及时发现系统中存在的安全漏洞和隐患。

根据扫描结果，制定详细的漏洞修复计划，及时修复系统漏洞，确保系统的安全性。

2.网络安全防护

加强系统的网络安全防护措施，配置防火墙、入侵检测系统、防病毒软件等安全设备，防止外部网络攻击和恶意软件入侵。

同时，定期检查网络安全设备的运行状态和配置情况，及时更新安全策略，确保网络安全防护措施的有效性。

3.数据安全保护

采取数据加密、访问控制、数据备份等措施，加强对系统中敏感数据的保护。确保数据在存储、传输和使用过程中的安全性，防止数据泄露、篡改和丢失。

同时，定期对数据安全保护措施进行评估和测试，及时发现并解决数据安全问题。

4.安全管理制度建设

建立完善的的安全管理制度，规范系统的安全管理流程和操作规范。包括用户账号管理、权限分配、数据备份与恢复、安全审计等方面，确保系统的安全管理有章可循、有据可依。

同时，加强对运维人员的安全意识培训，提高运维人员的安全管理水平和操作技能。

4.3.2.1.4.2服务成果

1.《广东省国土空间用途管制综合应用系统运维月度报告》：每月对系统的运维情况进行总结，为系统的持续优化和改进提供依据。

- 2.《广东省国土空间用途管制综合应用系统故障处理报告》（按需提供）：对于系统出现的故障，详细记录故障现象、故障原因、处理过程、解决方案等内容，形成故障处理报告，便于后续分析和总结经验教训。
- 3.《广东省国土空间用途管制综合应用系统年度运维服务总结报告》：在服务年度结束后，对全年的运维工作进行全面总结，为下一阶段的运维工作提供参考。

4.3.2.1.5广东省自然资源市场与资产监管综合应用运行维护服务

4.3.2.1.5.1广东省自然资源市场与开发利用监测监管子系统运行维护服务

4.3.2.1.5.1.1服务内容

运维内容包括软件系统检查、参数及数据故障排除、系统日常运维、故障排除、业务功能维护、软件升级、技术支持、高级技术专家服务等服务。

4.3.2.1.5.1.1.1软件系统检查

对广东省自然资源市场与开发利用监测监管子系统提供定期巡检服务，对软件提供系统性能测试，同时对影响软件系统的问题进行性能、参数等调整，从而达到优化目的。

软件系统检查主要包括如下几点：

1.性能评估

业务系统的响应性能状况

业务系统的响应性能指的是在正常业务并发负载下，以响应时间为主要关注点的业务模块操作的执行时间，通常单位为秒；

业务系统的稳定性性能状况

业务系统的稳定性性能的主要关注点则是在长时间较大负载压力下，业务系统能够正常完成业务操作的程度；

业务容量性能状况

业务容量性能状况指的是当前业务系统负载承受能力，目的是了解系统的业务压力可承受的范围，以便在峰值到来之前做出应对措施，通常关注的性能指标为并发量和业务的吞吐量。

2.业务连续性

(1)备份和恢复完整性

备份和恢复完整性实现 IT 系统内部对业务数据平台的保护。包括服务器和存储层相关技术。

备份完整性涉及的技术主要包括基于磁带、光盘等离线介质的备份技术(或称定点 拷贝);以及基于在线存储介质(磁盘)进行的生产数据快照技术。

实现备份完整性目标，首先需要映射业务种类所需要的数据集。即根据容灾备份系统的需求，明确哪些业务状态数据需要备份，事实上，需要提供最完善备份的是稳定的业务状态数据，而处理流程当中的中间临时数据的备份需求较低。

另外，在备份完整性的实施过程中，应该区分备份数据和存档数据。备份数据是为满足容灾备份的要求，具有较短的时效性，备份数据会根据一定的备份频度被反复覆盖。存档数据则按照业务或法规的要求，有较长的时效性，并具有不断累积的特性。

在绝大多数数据中心应用场合，备份是经常性的工作，恢复是十分偶然的操作，因此，恢复往往是难以经过充分巡检、优化的容灾备份技术--这就更加要求恢复操作具有明确的可预见性。

(2)信息完整性

信息完整性实现对业务数据平台的跨 IDC生产中心的保护，实现信息完整性技术是将业务连续性扩展到容灾阶段的一个十分关键的步骤。

信息完整性技术将生产中心的业务状态数据完整地复制到备份中心。

实现信息完整性可以采用同步或异步复制技术。

(3)处理完整性

处理完整性即对业务支撑系统平台的完整的、跨越生产中心的保护。

实现处理完整性，需要比较复杂的系统集成工作，包括详细的系统设计和规划。目前的大多数关键业务及其关联子业务系统的容灾的级别要

求为处理完整性。

实现处理完整性的关键在于以下三个要素：

一是对数据平台的保护—远程数据复制技术(即信息完整性)和对业务平台的保护—服务器、数据库等冗余及切换技术以及应用软件切换技术的集成；

二是对接入平台的保护和切换—外部接口的冗余和切换；

三是系统的监控和切换。

(4)业务连续性管理

业务连续性管理是IT信息安全政策的宏观管理文件，该规范清楚说明业务连续性计划对于保障信息安全所采取态度、监管责任以及信念。

业务连续性管理规范包含《灾难恢复预案》、《业务连续性计划》等文件。这些规范从宏观层面，涵盖了灾难备份建设所涉及的内容，其目的是要保护信息安全。根据 这些规范，建立业务连续性计划、灾难恢复预案，其中主要包括：灾难应急小组的组织 架构和人员职责，应急队伍、联络清单及各类应急处理流程，普及教育及人员培训计划和演习计划等，并报主管部门备案。

主管部门要对各单位灾难恢复预案进行全面审核，评估灾难恢复预案的完整性和可操作性，配合建立规范的管理制度和操作文档。

定期进行灾难演习与应急培训等多方面巡检内容。

3.运行状态检查

要求对广东省自然资源市场与开发利用监测监管子系统提供运行状态检查服务，针对用户数据 持续增加、系统运行缓慢等问题，需要定期对系统的运行环境进行监控。

(1)为确保系统能够稳定运行，需要定期对系统的运行环境进行监控。提供专业化程度高的技术服务工程师负责系统管理及数据库性能优化等技术支持服务，通过对系统的定期监控，及时了解系统的使用情况、运行情况并做好相应调整。

(2)对系统现状、配置与性能等进行检测和诊断，找出系统运行状态相关瓶颈，

通过掌握系统运行状况、系统资源使用情况及时开展有针对性的硬件、软件配置性能优化；掌握系统资源的使用情况，了解系统的执行效率。

(3)达到合理的硬件和软件配置，使系统资源使用达到平衡与性能提升。

4.3.2.1.5.1.1.2参数及数据故障排除

对广东省自然资源市场与开发利用监测监管子系统的软件系统提供备份服务：

1.软件升级版本时，会对整个应用系统进行备份，并实时跟进应用服务的运行情况。

2.更新某一个功能模块的微服务包 或 前端 程序包，要求对每个更新的程序以“微服务或前端程序包名称”+日期的方式进行备份，并登记功能更新日志和备份记录，出现问题可及时恢复。

3.数据库文件每天、每月、每年进行备份。

4.3.2.1.5.1.1.3系统日常运维

要求对广东省自然资源市场与开发利用监测监管子系统的软件系统提供日常维护服务。制定日常维护方案，针对业务接口、操作权限、系统资源和业务保障等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，周期性开展常规维护保养工作，消除故障异常、软件告警、存在问题和安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够7×24小时正常运行。

维护对象为应用程序，同时按照标准规范对软件系统进行管理，定期形成系统运行简报。具体维护内容如下：

1. 对接与自然资源部的土地市场动态监测与监管系统之间的功能同步升级

(1)自然资源部的土地市场动态监测与监管系统原有功能根据科室主管业务需要进行调整，

广东省需要把功能重新挂载到广东省自然资源市场与开发利用监测监管子系统中，与自然资源部的土地市场动态监测与监管系统保持业务数据上的一致性。

(2)自然资源部的土地市场动态监测与监管系统开发新的业务模块，广东省需要把这项功能加载到广东省自然资源市场与开发利用监测监管子系统中，并根据广东省自身情况进行调整，其中会涉及办件提醒或办件审核箱整合，为采购人提供方便快捷的功能。

(3)自然资源部有新任务下达到各省，广东省根据自身需要进行开发建设新业务模块，并与自然资源部的土地市场动态监测与监管系统做好接口对接和对接功能开发与调试，完成下达的任务指标。

2. 与广东省自然资源厅门户网之间的数据同步更新，提供共享数据。

广东省自然资源市场与开发利用监测监管子系统供应计划、出让公告、成交公示、供应结果、划拨合同和其他公告信息会公布到广东省自然资源厅门户网平台上，每月同步的数据量达到4000左右，安排人员每天按时检查同步程序是否正常运行，并对同步过程中出现的问题进行排查与修缮。

3. 更新部巡查系统之间的数据对接，同步动态巡查超期未巡查和闲置土地未巡查列表，及时发现问题进行排查和处理：

(1)开发利用的土地都需要进行闲置地、开竣工等任务巡查，部里自动按期下发项目巡查任务，广东省每天自动把巡查任务通过程序获取回来，再由市级分配任务，其中要监管任务获取程序的正常运行，并对同步过程中出现的问题进行排查与修缮，保证巡查任务的正常运行。

(2)根据广东省自身需要把巡查任务分级别等级进行区分提醒，超期未巡查和闲置地未巡查的任务是优先进行处理的，其中要实时监控超期未巡查任务和闲置地任务数据的获取，并对从部里超期未巡查和闲置地的数据通过同步程序实时进行更新。

4. 更新与省国土资源在线巡查系统之间的数据对接、巡查材料同步

(1)市级支配巡查组并把巡查任务分配到巡查组后进行任务发送，任务发送是通过广东省自然资源市场与开发利用监测监管子系统每天定时把巡查任务推送到省国土资源在线巡

查系统，并展示在在线任务列表中，其中要监控任务推送的情况，并排除推送失败发生的问题。

(2)各个地区去实地勘测后把巡查结果(附加巡查图片)上传到省国土资源在线巡查系统，广东省自然资源市场与开发利用监测监管子系统按时获取巡查结果和巡查图片，监控获取巡查结果和巡查图片程序中遇到的问题并及时处理。

5. 及时动态更新失信行为联合惩戒名单

对失信的纳税人导入到惩戒名单中，这部分人是不允许签订合同的。

4.3.2.1.5.1.1.4故障排除

要求对广东省自然资源市场与开发利用监测监管子系统提供故障处理服务。当发生故障时，按照故障定级和处理流程，及时响应，快速抢通故障点，尽早恢复业务，将故障对业务所造成的负面影响降到最低。在处理完毕后清理现场，提供故障处理简报。具体故障处理如下：

1.广东省自然资源市场与开发利用监测监管子系统服务出现无法启动时，提前做好各类需安装程序，将配置文件备份后，重新安装。

2.网络或系统相关服务器出现网络流量异常或服务器登录异常，判断服务器是否异常，检查网络流量，流量异常小则报修网络乙方，流量异常大则查杀病毒。

3.账号密码登录错误，检查账号密码是否有错误或重新分配。

4.系统未响应或无法访问，关闭系统，重新访问；检查系统访问地址是否有误，网络是否正常，端口是否正常，服务器是否正常开启。

5.系统反应缓慢，检测机器性能是否因过低而引起。

6.系统端口或数据库端口不通，检测端口是否被占用，更换端口。

4.3.2.1.5.1.1.5业务功能维护

要求对系统提供业务保障服务。应用系统业务保障是业务正常办理的关键内容，也是制约系统应用及发展水平的关键因素，要求管理和维护人员既要熟悉各类业务，又要熟悉相应应用系统的使用及维护，起到工程应用单位和系统开发单位之间的纽带作用。重点在以下几方面加强管理和维护，使系统能够高效而安全的运行：

1.业务功能维护：

(1)应用系统软件的升级性的保障服务，包括表单增加、审批变化、流程更改、改版/升级等。

(2)应用系统技术支持，包括人员权限、数据校正与修改等方面的使用维护。

(3)根据要求把广东省自然资源市场与开发利用监测监管子系统中有涉及新加或更新的功能内容添加到系统操作手册中。

(4)完善系统操作指引功能，方便各地区迅速找到自己负责的业务模块，了解一些基础规则并录入正确的业务数据，来提高工作效率。

(5)对接与部土地市场动态监测与监管系统之间的功能同步升级；

(6)与广东省自然资源厅门户网之间的数据同步更新，提供共享数据；

(7)更新部巡查系统之间的数据对接，同步动态巡查超期未巡查和闲置土地未巡查列表，及时发现问题进行排查和处理；

(8)更新与省国土资源在线巡查系统之间的数据对接、巡查材料同步；

(9)及时动态更新失信行为联合惩戒名单；

(10)每年按时更新批准建设用地批文的坐标并进行更新入库，提供分析数据依据；

(11)每天查检部省数据一致性的问题并及时反映处理；

(12)完善功能模块：土地管理信用模块，土地交易数据管理功能，集体建设用地 数据填报、统计、分析功能，土地出让过程监管模块等其他模块。

(13)根据业务协调要求调整设计相关的共享接口并配置安全相关策略和共享机制权限控制开放。

2.业务功能分析优化

对广东省自然资源厅的测绘地理信息监管与服务平台提供改造服务，针对应用系统的代码功能缺陷，或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求，提供系统迭代服务。

(1)业务系统功能代码优化，协助完成业务系统升级或变更。

(2)业务系统流程升级或改造，协助完成业务系统变更。

(3)业务系统程序逻辑改进，协助完成业务系统变更。

4.3.2.1.5.1.1.6软件升级

对广东省自然资源市场与开发利用监测监管子系统发布服务。制定标准流程、严格按流程进行版本更新发布。遵循发起变更申请---方案评审--
-备份、更新---验收的大致流程。

4.3.2.1.5.1.1.7技术支持

要求对广东省自然资源市场与开发利用监测监管子系统的软件系统提供响应支持服务及通信支持服务，为解决土地市场不同地区不同问题，建立统一的信息交流平台，提供7×24小时的热线服务，出现业务上或操作的问题时，专业人员给予解答和远程协助，紧急事件紧急处理，系统出现重大故障会安排技术人员现场处理，保证业务系统能够正常运行。

1.安排专业人员跟踪信息服务群中的问题并及时给予解答和处理，必要时远程进行协助。

2.针对科室临时统计的需求数据进行分析整理并给出相应的数据报表；

3.根据信息服务群提出的问题点分优先级一一登记，把任务分配到指定人员进行处理，并把处理结果及时反馈给各单位；

4.经过科室主管部门通过的各地方提出的临时需求数据给出相应的统计数据。

5.系统上出现紧急状况时会安排专业技术人员现场协助处理，并及时把处理结果进行反馈。

6.信息交流平台中有广东省自然资源厅主管领导在线监督，信息对内部公开。

4.3.2.1.5.1.1.8高级技术专家服务

对土地市场动态监测管理系统提供高级技术专家服务。咨询类型涵盖专项技术咨询、故障咨询、疑难问题分析等，咨询内容包括操作系统、中间件、业务流程、数据管理、性能瓶颈分析等等。

4.3.2.1.5.1.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.5.2广东省全民所有自然资源资产信息管理与监管子系统运行维护服务

4.3.2.1.5.2.1全民所有自然资源资产变更清查辅助模块

4.3.2.1.5.2.1.1服务内容

运维内容包括例行巡检、日常维护、漏洞（BUG）修复。

4.3.2.1.5.2.1.1.1例行巡检

定期对系统开展预防性维护服务（巡检），以确保系统的正常运行。通过定期对系统的各项性能指标进行测试，掌握系统使用的增长趋势，及时地升级系统软、硬件，调整系统参数，并为系统支撑平台的升级提供依据。

系统预防性维护主要包括以下内容（不限于）：

1.系统运行状态检查

应用服务与进程运行情况；

响应性能，测试关键功能响应时间。

2.功能完整性验证

核心功能测试：抽样验证高频使用功能（如打开工程、保存工程、清查变更变化量统计、汇交成功输出等）；

插件/模块兼容性：检查第三方插件或扩展功能是否正常。

3.日志与错误分析

收集并分类应用日志（Error/Warning级别），定位高频错误；

分析用户端崩溃文件。

4.更新与依赖管理

版本检查：确认当前版本是否为最新稳定版，检查补丁更新情况；

依赖项检查：验证运行时环境（如.Net运行时）兼容性。

4.3.2.1.5.2.1.1.2日常维护

要求制定日常维护方案，针对业务系统设定维护项，合理安排维护计划。在软件系统的正常运行过程中，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够正常运行。

具体维护内容如下：

1、技术支持

包括对用户日常操作指导，对因误操作导致的数据错误维护，对因系统功能缺失或缺陷导致问题的解答及处理等。

问题跟踪：建立问题分级响应机制；

用户反馈分析：定期汇总高频投诉问题。

2、系统功能维护

常规功能验证：定期抽样测试核心功能，检查自动化任务执行情况；

兼容性维护：监测新系统补丁影响；

异常处理：用户报障快速响应，常见问题知识库更新等。

3、更新管理

日常更新系统的补丁，清理冗余，不定期测试系统性能等，维护多版本共存时的兼容性。

4、文档维护

更新相关安装部署手册、维护故障处理手册；

修订用户操作手册、发布版本更新说明文档。

4.3.2.1.5.2.1.1.3漏洞（BUG）修复

1、漏洞发现与分类

通过人工审查的方式主动检测漏洞，结合用户反馈被动捕获问题，并按严重性和类型（安全、功能、性能等）分类分级。

2、修复流程规范化

按优先级排序（核心功能优先）、工单跟踪、设定SLA时效，技术层面采用热修复（紧急补丁）或版本迭代（完整测试），同步优化代码坏味道和升级依赖库。

3、测试与验证

严格验证修复效果，包括回归测试、灰度发布及用户验收，确保问题彻底解决。

4、预防与长效机制

通过根因分析（RCA）定位漏洞根源，管理技术债，制定开发规范（如安全编码指南），并建立知识库沉淀案例。团队协作需明确责任分工，定期培训复盘。最终目标是短期快速止损，长期通过流程优化和技术升级降低漏洞发生率，提升系统健壮性。

4.3.2.1.5.2.1.2服务成果

全民所有自然资源资产变更清查辅助模块运维周报；

全民所有自然资源资产变更清查辅助模块运维月报；

全民所有自然资源资产变更清查辅助模块运维年度总结报告；

全民所有自然资源资产变更清查辅助模块故障处理报告（按需提供）；

全民所有自然资源资产变更清查辅助模块需求确认单。

4.3.2.1.5.2.2全民所有自然资源资产变更清查成果质量检查模块

4.3.2.1.5.2.2.1服务内容

运维内容包括例行巡检、日常维护、漏洞（BUG）修复。

4.3.2.1.5.2.2.1.1例行巡检

定期对系统开展预防性维护服务（巡检），以确保系统的正常运行。通过定期对系统的各项性能指标进行测试，掌握系统使用的增长趋势，及时地升级系统软、硬件，调整系统参数，并为系统支撑平台的升级提供依据。

系统预防性维护主要包括以下内容（不限于）：

1.系统运行状态检查

应用服务与进程运行情况；

响应性能，测试关键功能响应时间。

2.功能完整性验证

核心功能测试：抽样验证高频使用功能（如变更清查成果签收、变更清查初检、自动全检等）；

插件/模块兼容性：检查第三方插件或扩展功能是否正常。

3.日志与错误分析

收集并分类应用日志（Error/Warning级别），定位高频错误；

分析用户端崩溃文件。

4.更新与依赖管理

版本检查：确认当前版本是否为最新稳定版，检查补丁更新情况；

依赖项检查：验证运行时环境（如.Net运行时）兼容性。

4.3.2.1.5.2.2.1.2日常维护

要求制定日常维护方案，针对系统进程、系统资源等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够正常运行。

具体维护内容如下：

1、技术支持

包括对用户日常操作指导，对因误操作导致的数据错误维护，对因系统功能缺失或缺陷导致问题的解答及处理等。

问题跟踪：建立问题分级响应机制；

用户反馈分析：定期汇总高频投诉问题。

2、系统功能维护

常规功能验证：定期抽样测试核心功能，检查自动化任务执行情况；

兼容性维护：监测新系统补丁影响；

异常处理：用户报障快速响应，常见问题知识库更新等。

3、更新管理

日常更新系统的补丁，清理冗余，不定期测试系统性能等，维护多版本共存时的兼容性。

4、文档维护

更新相关安装部署手册、维护故障处理手册；

修订用户操作手册、发布版本更新说明文档。

4.3.2.1.5.2.2.1.3漏洞（BUG）修复

1、漏洞发现与分类

通过人工审查的方式主动检测漏洞，结合用户反馈被动捕获问题，并按严重性和类型（安全、功能、性能等）分类分级。

2、修复流程规范化

按优先级排序（核心功能优先）、工单跟踪、设定SLA时效，技术层面采用热修复（紧急补丁）或版本迭代（完整测试），同步优化代码坏味道和升级依赖库。

3、测试与验证

严格验证修复效果，包括回归测试、灰度发布及用户验收，确保问题彻底解决。

4、预防与长效机制

通过根因分析（RCA）定位漏洞根源，管理技术债，制定开发规范（如安全编码指南），并建立知识库沉淀案例。团队协作需明确责任分工，定期培训复盘。最终目标是短期快速止损，长期通过流程优化和技术升级降低漏洞发生率，提升系统健壮性。

4.3.2.1.5.2.2.2服务成果

全民所有自然资源资产变更清查成果质量检查模块运维周报；

全民所有自然资源资产变更清查成果质量检查模块运维月报；

全民所有自然资源资产变更清查成果质量检查模块运维年度总结报告；

全民所有自然资源资产变更清查成果质量检查模块故障处理报告（按需提供）；

全民所有自然资源资产变更清查成果质量检查模块需求确认单。

4.3.2.1.5.2.3全民所有自然资源资产信息管理监管模块

4.3.2.1.5.2.3.1服务内容

运维内容包括例行巡检、日常维护、故障处理、安全加固、2026年资源自然在线清查业务辅助支持及功能优化等。

4.3.2.1.5.2.3.1.1例行巡检

包括对广东省全民所有自然资源资产信息管理与监管子系统全民所有自然资源资产变更清查辅助模块、全民所有自然资源资产变更清查成果质量检查模块、全民所有自然资源资产信息管理监管模块各个版块检查，保证功能和模块运行正常；用户数量及角色检查，维护账户权限，清除测试账号、僵尸账号；应用系统冗余及缓存检查，保证系统运行速率。

4.3.2.1.5.2.3.1.2日常维护

要求制定日常维护方案，针对系统进程、系统接口、系统权限、系统资源等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够正常运行。

具体维护内容如下：

(1)技术支持

包括对省、市级用户日常操作指导，对因误操作导致的数据错误维护，对因系统功能缺失或缺陷导致问题的解答及处理等。

(2)日志检查服务

通过日志管理系统或其他数据库查询手段检查系统运行情况，及时发现执行路径异常、参数和性能异常，为系统正常运行提供保障。

(3)应用系统维护

针对B/S系统，管理各板块，维护各板块数据。按要求增加、变更、删除、备份数据。

4.3.2.1.5.2.3.1.3安全加固

配合相关部门对系统进行安全扫描，及时修复系统漏洞，升级、更新中间件，处理安全隐患，保证系统安全。具体涵盖如下几个方面：

1.系统漏洞扫描与修复

定期对全民所有自然资源资产信息管理监管模块进行全面的安全漏洞扫描，及时发现系统中存在的安全漏洞和隐患。

根据扫描结果，制定详细的漏洞修复计划，及时修复系统漏洞，确保系统的安全性。

2.网络安全防护

加强系统的网络安全防护措施，配置防火墙、入侵检测系统、防病毒软件等安全设备，防止外部网络攻击和恶意软件入侵。

同时，定期检查网络安全设备的运行状态和配置情况，及时更新安全策略，确保网络安全防护措施的有效性。

3.数据安全保护

采取数据加密、访问控制、数据备份等措施，加强对系统中敏感数据的保护。确保数据在存储、传输和使用过程中的安全性，防止数据泄露、篡改和丢失。

同时，定期对数据安全保护措施进行评估和测试，及时发现并解决数据安全问题。

4.安全管理制度建设

建立完善的安全管理制度，规范系统的安全管理流程和操作规范。包括用户账号管理、权限分配、数据备份与恢复、安全审计等方面，确保系统的安全管理有章可循、有据可依。

同时，加强对运维人员的安全意识培训，提高运维人员的安全管理水平和操作技能。

4.3.2.1.5.2.3.1.4故障处理

对系统功能缺陷如业务办理失败、数据上报失败、统计结果偏差、流程异常、安全缺陷等问题提供系统缺陷（BUG）修复服务，包括缺陷复现、代码分析、测试验证及生产环境发布验证，具体如下：

1、缺陷复现

依据用户反馈或测试报告的操作步骤在测试环境（预发布环境）执行复现，详细记录每一步操作及系统响应，形成复现报告，清晰界定缺陷表现形式与触发条件。

2、代码分析

运用代码调试工具和日志分析手段，结合复现报告，精准定位导致缺陷的代码位置和逻辑错误。深入分析代码错误产生的原因，如业务逻辑错误、数据边界处理不当、接口调用异常等，并评估该缺陷对系统其他功能模块可能产生的影响。

3、修复实施与测试验证

按照修复方案进行代码修改，遵循代码规范和版本控制流程，保证代码的可维护性与可追溯性。修改完后依次开展系统测试，模拟生产环境进行全面测试，验证系统在各种业务场景下的稳定性与可靠性。

生产环境发布验证

制定详细的发布计划，明确发布时间、发布步骤、回滚方案等，对修复后的代码进行打包和部署前的最终检查，确保发布准备充分；然后按照发布计划，在生产环境进行代码发布。发布过程中密切监控系统运行状态，及时处理可能出现的问题；发布完成后，对系统进行全面验证，确保缺陷已完全修复，系统功能恢复正常。收集用户反馈，评估修复效果，为后续优化提供依据。

4.3.2.1.5.2.3.1.5 2026年资源自然在线清查业务辅助支持及功能优化

开展2026年资源自然在线清查业务。

- (1) 根据2026年资产清查成果数据标准调整数据接入标准，保障资产清查数据的正常接入。
- (2) 进行资产清查数据接入的核查，包括接入数据的质量检查、数量核实等。
- (3) 资产在线清查过程中，为各地市、区县资产在线清查信息填写提供技术支持，包括系统操作答疑、资产清查填写规范指导等。
- (4) 解决在线清查过程中因数据填报产生的功能异常，同步优化相关功能，提高系统的稳定性和灵活性。
- (5) 开展自然资源资产实物量 and 价值量成果检查工作，保证在线清查成果质量。

4.3.2.1.5.2.3.2服务成果

广东省全民所有自然资源资产信息管理监管模块运维服务周报

广东省全民所有自然资源资产信息管理监管模块运维巡检月报

广东省全民所有自然资源资产信息管理监管模块整改报告（按需提供）；

广东省全民所有自然资源资产信息管理监管模块运维服务总结报告。

4.3.2.1.6广东省测绘地理信息管理综合应用运行维护服务

4.3.2.1.6.1广东省测绘地理信息监管与服务系统运行维护服务

4.3.2.1.6.1.1服务内容

运维内容包括现场巡检、软件维护、日常维护、技术支持、问题处理、业务支撑、软件备份、安全加固、版本更新发布等。

4.3.2.1.6.1.1.1现场巡检

对广东省测绘地理信息监管与服务系统提供定期巡检服务。

1.应用系统巡检：

- (1) 应用服务进程运行情况、进程连接数、服务的正常启停；
- (2) 应用服务参数配置更新前是否备份，日常日志是否按时清理；
- (3) 应用服务系统文件、应用程序、数据的备份与清理；
- (4) 灾备情况检查。

2.应用服务器巡检：

CPU利用率、内存使用情况、硬盘存储使用情况、网络连接情况、操作系统版本。

4.3.2.1.6.1.1.2软件维护

对广东省测绘地理信息监管与服务系统提供日常维护服务。建立切实可行的运行维护体系相关制度，保障系统的日常管理和运行维护。实时解决采购人提出的各种系统使用问题，保证系统的正常运行，对软件系统进行日常的运行状态监控，同时能够对系统的运行数据进行记录，对安全事件的发生原因进行判断和解决。软件系统维护主要有三种类型：

- 1.改进在特定的使用条件下暴露出来的一些潜在程序错误或设计缺陷。针对系统程序错误及时派专业技术开发人员进行修改排查，设计缺陷将整体评估系统风险进行排查修复，保障系统顺利运行。
- 2.因在软件使用过程中数据环境发生变化（例如一个事务处理代码发生改变）或处理环境发生变化（例如安装了新的硬件或操作系统），需要修改软件以适应这种变化。针对新加入系统和软件，从系统运行稳定性整体考虑，在不影响现有系统和业务运行的情况下进行软件修改完善。
- 3.用户在使用过程中提出改进现有功能，以及改善总体性能的要求，需要修改或升级软件以满足用户需求。在维护期内，根据成熟产品的软件开发版本，对已有系统进行升级更新，提升整体系统性能和用户体验。

4.3.2.1.6.1.1.3日常维护

对系统提供日常系统运维服务，开展广东省测绘地理信息监管与服务系统日常运维工作，包括但不限于系统用户账号配置管理、电子证照与电子印章维护更新、审查审批业务规则维护更新、业务数据维护更新、统计查询技术支持服务等。

4.3.2.1.6.1.1.4技术支持

对广东省测绘地理信息监管与服务系统提供响应支持服务。

- 1.负责服务请求、告警监控、时间等的响应和处理，包括热线接听、使用问题处理、告警监控、知识库维护等内容。
- 2.建立服务请求管理分类分级机制，根据潜在影响程度建立回溯机制；将响应支持过程中产生的文档、记录等及时归档。
- 3.在服务请求关闭时，启用变更管理流程，保证相关记录与信息系统运行配置相一致。

4.3.2.1.6.1.1.5问题处理

对广东省测绘地理信息监管与服务系统提供故障处理服务。常见软件故障有：浏览器故障（发送错误报告、发生内部错误窗口关闭、出现运行错误、无法打开新窗口、互联网状态下无法打开某些站点、浏览器无法重新安装等）、终端冲突问题、蓝屏死机问题、系统无法启动、系统文件解析、流氓软件问题。

4.3.2.1.6.1.1.6业务支撑

运用标准化运维体系，对业务系统提供业务架构、环境部署、监控、软件升级和技术支持等多方面业务运维服务。发挥支撑和保障作用。

4.3.2.1.6.1.1.7软件备份

对广东省测绘地理信息监管与服务系统提供备份服务。制定备份方案，根据具体情况对应用系统及数据进行备份。备份情景有软件升级备份、灾备备份、日常备份等等。备份内容主要包括：数据备份、软件运行环境及中间件、库文件和操作系统配置备份等等。

4.3.2.1.6.1.1.8安全加固

对广东省测绘地理信息监管与服务系统提供安全加固服务，及时修复系统漏洞，升级、更新中间件，处理安全隐患，保证系统安全。

4.3.2.1.6.1.1.9版本更新发布

对广东省测绘地理信息监管与服务系统提供系统发布服务，主要是对系统运行所需IT资源进行调整与系统发布。

- 1.根据版本发布、系统调整等需求，填写变更单，发起变更申请。
- 2.对变更的方案进行评审，填写操作步骤和回滚方案等，提交上级审批。
- 3.审批通过后判断是否需要审批变更方案。
- 4.变更实施完毕，更新和维护备份策略，组织相关人员进行验收。

4.3.2.1.6.1.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.6.2天地图·广东子系统运行维护服务

4.3.2.1.6.2.1服务内容

运维内容包括日常维护、例行巡检、技术支持、故障处理等。

4.3.2.1.6.2.1.1日常维护

制定日常维护方案，针对业务系统设定维护项，合理安排维护计划，实施日常维护工作。在软件系统的正常运行过程中，消除系统缺陷、故障异常、软件告警、报错、存在问题等，保障软件系统运行状况良好；消除安全问题，降低数据缺失风险与负面影响，确保软件系统能够安全运行。

具体维护内容如下：

(1)日志检查服务

通过日志管理系统或其他查询手段检查系统运行情况，及时发现系统运行过程中的问题，包括但不限于执行路径异常、参数和性能异常等，为系统正常运行提供保障。

(2)应用系统维护

- 1.监控日常运行状态，跟踪系统功能模块及时处理异常情况；管理各模块，维护各模块的接口、 workflow、计算模型、任务和数据。按要求对

workflow、计算模型、任务和数据进行增加、变更、删除、备份。

2.系统缺陷修复优化，对系统的缺陷和漏洞进行定期检查，按要求对系统缺陷进行修复和优化。

3.系统性能优化，在系统使用过程中由系统缺陷、网络、资源瓶颈等情况产生的性能问题，定期开展性能测试评估，制定性能优化方案，实施性能优化工作。

4.系统适配升级，根据操作系统、数据库、中间件、大数据平台等部署环境的升级情况，及时对系统进行对应的适配改造，保障系统稳定运行。

4.3.2.1.6.2.1.2例行巡检

定期对系统开展预防性维护服务（巡检），以确保系统的正常运行。通过定期对系统的各项性能指标进行测试，掌握系统使用的增长趋势，及时地升级系统软、硬件，调整系统参数，并为系统支撑平台的升级提供依据。

系统预防性维护主要包括以下内容（不限于）：

1.系统状态检查

u应用服务进程运行情况、进程连接数。

u数据库运行状态分析、中间件运行状态分析。

u网络流量统计、协议分布、出错率统计。

u应用的各种接口、workflow、计算模型、任务。

2.用户行为检查

用户系统访问行为。

用户在系统上的增删改行为。

用户对数据库的操作行为。

4.3.2.1.6.2.1.3技术支持

1.协助开展系统组件测试、部署和新模块接入等工作。在有新的应用系统需要接入天地图·广东子系统时，提供新对象接入调试服务，使得新的对象纳入系统管理。

2.对天地图·广东子系统提供改造服务，针对应用系统的代码功能缺陷，或广东省自然资源厅由于故障、迁移、安全等要求提出的升级改造需求，提供系统迭代服务。

3.系统功能代码优化，协助完成系统升级或变更。

4.针对系统中各类查询统计报表功能的完善、调整、配置及维护。主要对存在特殊要求的且系统已有查询或汇总分析功能不满足统计分析需求的，提供技术分析、数据辅助查询、安全事件建模、数据关联输出等技术支持服务。

5.在两会、国庆或网络安全重点保障期间，保障系统的正常运行，为安全调查分析人员开展网络安全保障监控提供应急支持服务，保障系统的正常运行。

4.3.2.1.6.2.1.4故障处理

对系统功能缺陷如业务办理失败、数据上报失败、统计结果偏差、流程异常、安全缺陷等问题提供系统缺陷（BUG）修复服务，包括缺陷复现、代码分析、测试验证及生产环境发布验证，具体如下：

1、缺陷复现

依据用户反馈或测试报告的操作步骤在测试环境（预发布环境）执行复现，详细记录每一步操作及系统响应，形成复现报告，清晰界定缺陷表现形式与触发条件。

2、代码分析

运用代码调试工具和日志分析手段，结合复现报告，精准定位导致缺陷的代码位置和逻辑错误。深入分析代码错误产生的原因，如业务逻辑错误、数据边界处理不当、接口调用异常等，并评估该缺陷对系统其他功能模块可能产生的影响。

3、修复实施与测试验证

按照修复方案进行代码修改，遵循代码规范和版本控制流程，保证代码的可维护性与可追溯性。修改完后依次开展系统测试，模拟生产环境进行全面测试，验证系统在各种业务场景下的稳定性与可靠性。

生产环境发布验证

制定详细的发布计划，明确发布时间、发布步骤、回滚方案等，对修复后的代码进行打包和部署前的最终检查，确保发布准备充分；然后按照发布计划，在生产环境进行代码发布。发布过程中密切监控系统运行状态，及时处理可能出现的问题；发布完成后，对系统进行全面验证，确保缺陷已完全修复，系统功能恢复正常。收集用户反馈，评估修复效果，为后续优化提供依据。

4.3.2.1.6.2.2服务成果

系统月度巡检报告，内容需包括例行巡检内容；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.6.3广东省遥感影像管理与服务子系统（卫星遥感影像管理与服务）运行维护服务

4.3.2.1.6.3.1服务内容

运维内容包括日常维护、故障处理、业务保障、安全加固等。

4.3.2.1.6.3.1.1日常维护

1.提供系统运行监控

用管理员账号登录系统查看系统操作日志，通过日志查看是否有非法的数据删除、异常登入、登出操作等信息。定期查看系统日志，操作日志，判断是否有运行错误信息。

2.提供用户访问管理服务

信息系统的用户管理服务，包括：用户账户、权限、组织架构的新增、变更、删除。依据流程分配软件系统的账号和权限，权限以最小原则分配，并对登录日志和权限进行定期审查。根据接入管理的标准规范，设置密码复杂度和登录次数限制等规则。

3.提供日志管理与分析服务

定期登录堡垒机查看服务器情况，通过TKE的web端查看容器日志，通过对系统日志进行巡查、抽查和定向检查，提早发现执行路径异常、参数和性能异常。

4.提供资源统计与报表生成服务

统计平台中所包含的物理机、虚拟机、存储、网络等资源信息；统计各类资源的用户使用量、每类资源的使用情况，如业务系统的CPU、内存、存储、IP的资源总量及占用量。按照天、周、月、季度的频率周期性生成报表。

5.、配置管理与维护

针对不同需求和安全规则进行用户配置管理、系统配置管理和维护。

4.3.2.1.6.3.1.2故障处理

1.应用软件故障处理

在系统存在无法访问、响应超时、系统报错等情况下进行及时响应，确保系统持续正常运行。

2.网络与服务器故障处理

查看服务器或客户端系统网络状态，查看服务端口是否正常开启。如无法解决联系网络维护人员或网络供应商解决。

3.数据接口故障处理

对于接口报错等故障进行维护解决，查看错误日志，记录出错信息并判断，确保从问题根源解决。

4.系统恢复措施

若出现操作系统或数据库故障，在采取任何措施之前,应该备份故障服务器上所有相关数据,并确定通过备份数据可以至少把服务器恢复到故障发生时的初始状态。

4.3.2.1.6.3.1.3业务保障

1.业务流程优化

应用系统软件的升级性的保障服务，包括操作流程优化、审批变化、流程更改、改版/升级等。系统功能交互体验层面优化，对系统便捷性不

足的功能进行升级优化。同时为系统新用户提供标准化操作培训、安装部署全流程指导等配套服务。

2.业务表单管理

针对系统教程配套的业务资料，提供实时同步的更新服务，严格规范工具升级补丁的管理流程，并第一时间上传至系统供用户下载使用。

3.系统性能优化

针对系统查询及数据入库等功能，开展性能测试与深度调优，并实施持续性的优化迭代更新。

4.业务支持

针对新增功能需求及时响应，系统评估改造成本、业务影响范围与工作量，并结合实际状况在规定期限内完成升级改造任务。

4.3.2.1.6.3.1.4安全加固

1.数据安全保护

根据安全测评要求，及时修复系统漏洞，升级、更新中间件，处理安全隐患，保证系统安全。采取数据加密、访问控制、数据备份等措施，加强对系统中敏感数据的保护。确保卫星影像数据在存储、管理、传输和使用过程中的安全性，防止数据泄露、篡改和丢失。

2.安全管理制度建设

建立完善的的安全管理制度，规范系统的安全管理流程和操作规范。包括用户账号管理、权限分配、数据备份与恢复、安全审计等方面，确保系统的安全管理有章可循、有据可依。

同时，加强对运维人员的安全意识培训，提高运维人员的安全管理水平和操作技能。

4.3.2.1.6.3.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.1.7广东省自然资源厅城市地质信息管理服务平台运行维护服务

4.3.2.1.7.1服务内容

运维内容包括例行巡检、日常维护、响应支持、故障处理、安全加固、系统备份、运行环境调优，服务地点为用户指定地点。

4.3.2.1.7.1.1例行巡检

(1)信息资产统计工作

了解现有的信息资产情况，更好的提供系统的运行维护服务。内容包括：租赁软件型号、数量、版本、补丁等信息统计记录；云服务器数量、系统版本、安装软件情况记录；应用软件及WEB系统数量、版本、部署情况记录。

(2)网络运行巡检工作

包括对服务器及客户端网络的连通性、网络性能、网络监控检查。通过对网络运行状况、网络问题进行周期性检查、分析后，提出指导性建议。

(3)云服务器系统巡检服务

云服务器系统的巡检服务是对设备的监控记录查看，设备的运行状态监控查看，并进行故障处理，操作系统维护，补丁升级等内容。具体有CPU性能管理；内存使用情况管理；硬盘利用情况管理；系统进程管理；主机性能管理；主机系统文件系统管理；端口状态、传输速度；监控服务进程、备份情况(起止时间、是否成功、出错告警)；

(4)应用系统巡检工作

包括对平台的数据管理维护子系统、三维建模子系统、城市地质分析评价模型管理子系统等C/S应用系统，及广东省自然资源厅城市地质信息管理服务平台门户、地上地下二三维一体化管理分析子系统、地质信息综合展示平台、示范应用系统、城市地质公众服务子系统、服务发布与共享子系统、运行维护子系统等B/S系统各个版块检查，保证功能和模块运行正常；用户数量及角色检查，维护账户权限，清除测试账号、僵尸账号；应用系统冗余及缓存检查，保证系统运行速率。

(5)数据库巡检工作

数据库巡检工作包括对PostgreSQL、MongoDB、ElasticSearch、Hadoop数据库性能管理，数据库的主动性能管理对系统运维非常重

要。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生所在地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。

此外，巡检工作还包括快速发现、诊断和解决性能问题，在出现问题时，及时找出性能瓶颈，解决数据库性能问题，维护高效的应用系统。

(6)中间件巡检工作

中间件管理是指对tomcat、nginx等中间件的日常维护管理和监控工作，提高对中间件平台事件的分析解决能力，确保中间件平台持续稳定运行。中间件监控指标包括配置信息管理、故障监控、性能监控。

4.3.2.1.7.1.2日常维护

要求制定日常维护方案，针对系统进程、系统接口、系统权限、系统资源等方面设定维护项，合理安排维护计划。在软件系统的正常运行过程中，消除故障异常、软件告警、存在问题、安全隐患等，保障软件系统运行状况良好，防止故障发生，降低数据缺失风险与负面影响，确保软件系统能够正常运行。

具体维护内容如下：

(1)技术支持

包括对省、市级用户日常操作指导，对因误操作导致的数据错误维护，对因系统功能缺失或缺陷导致问题的解答及处理等。

(2)日志检查服务

通过日志管理系统或其他数据库查询手段检查系统运行情况，及时发现执行路径异常、参数和性能异常，为系统正常运行提供保障。

(3)应用系统维护

针对C/S系统，监控日常运行状态，跟踪常用功能模块及时处理异常情况；

针对B/S系统，管理各板块，维护各板块数据。按要求增加、变更、删除、备份数据。

(4)提供数据库维护服务

通过MapGIS大数据管理平台和数据库工具检查数据库实例、服务、监听状态，跟踪控制文件、在线日志、表空间、数据文件状态，着重关注数据回滚段。

(5)提供操作系统维护服务

日常更新系统的系统补丁，清理冗余，不定期测试系统性能等。

4.3.2.1.7.1.3响应支持

本平台中C/S专业系统面向地质行业专业人员，公众服务子系统面向互联网用户，针对日常咨询、故障问题等服务请求进行记录，根据事件的性质、类别、等级派相关人员进行处理，并对事件处理流程进行跟踪监督，确保服务请求得到及时的响应与处理。

4.3.2.1.7.1.4故障处理

要求对系统故障进行处理。根据系统故障大小等级建立响应机制，一般小故障可快速、简单处理的，由运维人员自行处理；费时、难度高、重要影响客户使用的故障，上报管理层，请求调度相关人员协助处理。

(1)网络故障。查看服务器或客户端系统网络状态，查看服务端口是否正常开启。如无法解决联系网络维护人员或网络供应商解决。

(2)服务器故障。服务器端软件无法使用,查看任务管理器和事件日志,记录出错的信息并判断。关闭相应的服务器进程,并重新启动该服务器进程.查看数据库连接是否正确.查看数据库服务器是否运行正常.如判定为服务器程序崩溃，请求重装程序。

(3)操作系统故障。经判断为服务器操作系统层面的故障后,在采取任何措施之前,应该备份故障服务器上所有相关数据,并确定通过备份数据可以至少把服务器恢复到故障发生时的初始状态(即保护现场),在确定任何一步操作有回复的途径之前,不应该进行该操作.查看任务管理器,记录资源使用状况以及各个进程详细情况,以备后续判断。

(4)数据库故障。备份所有的数据库文件,在确定每步操作可以有回复的途径之前,不宜进行该操作.查看操作系统的数据库服务,监听服务等是否正确启动,并重新启动这些服务.以上措施无效,重新启动数据库.如果为数据库数据文件损坏,则对使用数据库备份文件对数据进行回复操作.以上措施无效,备份数据库文件,删除数据库,重建数据库,然后导入备份的数据库文件。

4.3.2.1.7.1.5业务保障

要求对系统提供业务保障服务。系统包含的大部分子系统，专业性较强，使用难度较高，需要对用户进行专业指导培训。

4.3.2.1.7.1.6安全加固

配合相关部门对系统进行安全扫描，对安全整改意见及时响应处理。

4.3.2.1.7.1.7运行环境调优

要求对系统提供运行环境调优服务，针对系统数据持续增加、系统运行缓慢等问题，提供系统性能测试，并对操作系统、数据库系统、应用服务器进行调优。

(1)操作系统调优。当应用系统资源使用出现过占用或资源使用异常的情况，如CPU过高、内存不足、网络速率慢时候，申请增加服务器配置、升级补丁、调整网络拓扑结构。

(2)数据库系统优化。可增加物理设备，把数据区和索引区分开部署，控制数据库和用户数据库分别建立不同硬盘；临时库、系统库、日志库足够大，设置自行清除方案；设置合理锁资源，避免发生阻塞；调整数据库连接数以应对增加的用户数。

(3)应用系统优化。为JVM分配足够内存；合理配置线程，根据并发量设置合适数据库连接池；客户端连接超时或延缓时设置引擎调度器。

4.3.2.1.7.2服务成果

广东省自然资源厅城市地质信息管理服务平台运维服务周报；

广东省自然资源厅城市地质信息管理服务平台运维巡检月报；

广东省自然资源厅城市地质信息管理服务平台整改报告（按需提供）；

广东省自然资源厅城市地质信息管理服务平台运维服务总结报告。

4.3.2.1.8广东省国土资源技术中心政务服务综合保障子系统运行维护服务

4.3.2.1.8.1服务内容

运维内容包括日常维护、故障处理、业务保障、安全加固等。

4.3.2.1.8.1.1日常维护

1.提供业务维护服务

利用管理员账号登录系统查看系统操作日志，监控是否有非法的数据删除、异常登入、登出操作等信息。定期查看系统日志，操作日志，判断是否有运行错误信息，定期备份日志等操作。

2.提供访问管理服务

信息系统的用户管理服务，包括：用户账户、权限、组织架构的新增、变更、删除。依据流程分配软件系统的账号和权限，权限以最小原则分配，并对登录日志和权限进行定期审查。根据接入管理的标准规范，设置密码复杂度和登录次数限制等规则。

3.提供日志管理服务

对软件系统的日志采集、展现和检查分析。日志展现围绕资源的整个生命周期，体现资源的具体操作、操作时间、操作人、操作结果等信息。通过对系统日志进行巡查、抽查和定向检查，提早发现执行路径异常、参数和性能异常。

4.提供统计报表服务

统计平台中所包含的物理机、虚拟机、存储、网络等资源信息；统计各类资源的用户使用量、每类资源的使用情况，如业务系统的CPU、内存、存储、IP的资源总量及占用量。按照天、周、月、季度的频率周期性生成报表。

5.提供配置管理服务

使软件系统各种配置信息得到有效、完整、可追溯的记录归档和维护。配置信息包括：软件系统及其运行环境中所有IT设备、系统及其配置信息；各IT设备、系统之间的物理和逻辑关系。

6.提供数据库维护服务

针对数据库的可用性、完整性的检查维护；安装部署合理性，日志维护等。

7.提供中间件维护服务

全面维护中间件运行状况、性能分析，对采集的数据、中间件日志文件进行定期分析与检查；启动/停止中间件实例、查看/修改tomcat实例配置和启动参数、查看中间件实例日志、部署业务程序、设置/取消开机自启动等内容。

8.提供操作系统维护服务

更操作系统的系统补丁，清理冗余日志，不定期测试系统性能等。

4.3.2.1.8.1.2故障处理

要求对系统提供故障处理服务。当发生故障时，按照故障定级和处理流程，及时响应，快速抢通故障点，尽早恢复业务，将故障对业务所造成的负面影响降到最低。在处理完毕后清理现场,提供故障处理简报。具体故障处理如下：

- 1.应用软件出现无法启动软件可执行文件时，提前做好各类需维护软件安装程序，将应用软件数据文件备份后，重新安装。
- 2.应用软件打开过程中或运行中异常错误关闭，准备好安装程序，操作系统优化和修补软件，查杀病毒软件，判断出错原因，备份数据，采取相关修复措施。
- 3.操作系统出现系统异常或系统资源占用严重，应准备好系统检查程序及修补程序，以及查杀病毒软件，告知使用者错误原因可能类型，提出解决方案，经使用者认可后采取相应措施。
- 4.操作系统若为B/S 结构系统，浏览器异常或无法下载控件，应准备流氓软件清理程序、修复浏览器软件、查杀病毒软件，检查浏览器选项设置，分析原因进行修复。
- 5.网络或服务器出现网络流量异常或服务器登录异常（B/S结构系统），判断服务器是否异常，检查网络流量，流量异常小则报修网络服务商，流量异常大则查杀病毒。
- 6.账号密码登录错误，检查账号密码是否有错误或重新分配。
- 7.系统未响应或无法访问，关闭系统，重新访问；检查系统访问地址是否有误，网络是否正常，端口是否正常，服务器是否正常开启。
- 8.系统反应缓慢，检测机器性能是否因过低而引起。
- 9.系统端口或数据库端口不通，检测端口是否被占用，更换端口。

4.3.2.1.8.1.3业务保障

要求对系统提供业务保障服务。应用系统业务保障是业务正常办理的关键内容，也是制约系统应用及发展水平的关键因素，要求管理和维护人员既要熟悉各类业务，又要熟悉相应应用系统的使用及维护，起到工程应用单位和系统开发单位之间的纽带作用。重点在以下几方面加强管理和维护，使系统能够高效而安全的运行：

- 1.应用系统软件的升级性的保障服务，包括表单增加、审批变化、流程更改、改版/升级等。
- 2.应用系统技术支持，包括人员权限、数据校正与修改等方面的使用维护。

4.3.2.1.8.1.4安全加固

根据安全测评要求，及时修复系统漏洞，升级、更新中间件，处理安全隐患，保证系统安全。

4.3.2.1.8.2服务成果

系统月度巡检报告；

系统故障处理报告（按需提供）；

系统年度运维服务总结报告。

4.3.2.2业务系统支撑环境运行维护服务

为提高运维工作成效，对本项目的6个应用所部署的运行环境（指自然资源云专区）中的数据库、容器平台、分布式服务框架、NAS存储、OBS存储等进行统一运维。

6个应用：

广东省自然资源一体化数据库（自然资源三维时空数据库）运行维护服务；

广东省自然资源一体化管理与服务平台（国土空间基础信息平台）运行维护服务；

广东省自然资源和不动产登记综合应用运行维护服务；

广东省国土空间用途管制综合应用运行维护服务；

广东省自然资源市场与资产监管综合应用运行维护服务；

广东省测绘地理信息管理综合应用运行维护服务。

4.3.2.2.1自然资源云专区数据库实例运维服务

4.3.2.2.1.1服务内容

4.3.2.2.1.1.1业务适配

针对项目范围内的自然资源云专区数据库的业务场景进行业务适配时，所产生的数据库对象设计、适配问题排查、适配性问题指导，根据需求进行业务相关的功能测试验证等服务内容。

在自然资源厅相关业务系统进行迁移或者改造时，针对分布式数据库的产品特征可以提供针对性的指导建议的技术支持服务，使业务可以更大限度的利用分布式架构下的特点，并尽量规避因在使用集中数据库固定思维带来的具体问题，具体包括：

根据实际业务特征配合进行数据库对象的设计。

配合业务SQL设计，并根据技术标准和规范进行审核与建议。

配合对业务迁移或者改造过程中的问题排查，协助定位问题，使业务能够快速顺利进行。

4.3.2.2.1.1.2性能优化

提供数据库产品性能调优工作，包括：对数据库性能进行全面的分析，剖析数据库访问过程中存在的瓶颈，提出优化调整方案，配合用户实施、测试，提升数据库性能；

提供数据库产品优化改善工作，包括：对当前业务运行基础环境进行勘查，给出结合现有应用规模和业务运行状况的数据库相关优化建议，配合应用开发商完成SQL优化、PLSQL优化、配置优化、存储配置优化、存储空间资源管理优化等工作；

针对数据库适配场景交付过程中出现的瓶颈问题，根据数据库产品的特性，提供项目范围内的自然资源云专区数据库性能优化指导建议的技术支持服务。例如：优化慢查询，优化表结构等。

4.3.2.2.1.1.3技术咨询建议

在厅业务系统进行操作或改造时，提供项目范围内的自然资源云专区数据库的技术咨询指导建议服务。

在数据库交付期间，业务系统进行操作或改造时，根据数据库产品的特性，可以提供针对性的技术咨询指导建议服务，以此最大限度的利用数据库的特性，帮助系统尽量避免开发工作量大的问题。包括但不限于：用户权限管理、数据审计等。

4.3.2.2.1.1.4紧急救援服务

根据数据库系统故障对业务连续性的影响程度，按照所影响的类别、运行时段和影响程度分为四级，即一级故障（重大故障）、二级故障（严重故障）、三级故障（一般故障）和四级故障（一般事件），其定义和对应的现场响应要求如下表所示。

故障级别故障现象、电话响应、现场响应

一级故障数据库宕机或关键性数据库故障导致系统不可用立即响应，工程师2小时内到现场，2小时内恢复业务

二级故障数据库系统性能严重损坏，但数据库系统仍可正常运行立即响应，工程师2小时内到现场，4小时内恢复业务

三级故障数据库系统出现直接影响服务、导致性能或服务部分退化的故障立即响应，工程师2小时内到现场，6小时内恢复业务

四级故障数据库系统运行仅受到有限的影响或未受到严重影响立即响应，工程师3小时内到现场，8小时内解决故障。

4.3.2.2.1.1.5数据迁移服务

提供当前数据库类型、数据存储环境、数据量、数据对象勘查，提供数据迁移策略建议，提供存量数据和数据对象迁移服务，同时提供原数据库系统应用语句改写翻译，以及迁移后数据、应用检查校验配合工作。

4.3.2.2.1.1.6版本管理安全扫描及补丁升级服务

提供数据库产品版本和环境勘查，产品升级策略建议，小版本升级or补丁包更新安装部署工作，以及产品升级后验证工作；

服务商提供数据库版本的管理，增打补丁的需求，使增打补丁后的数据库环境能够安全稳定正常运作，有效支撑业务应用系统。定期提供所发布的相关软件更新和补丁情况，及时通知影响系统安全运行的软件漏洞和修补方法，并提供相应的现场服务。提供全方位的安全策略评估，并提出改进意见。此外，提供杀毒软件部署，及时升级软件和病毒库，定期开展杀毒和安全扫描。

4.3.2.2.1.2服务成果

月度巡检报告；

月度故障处理报告（按需提供）；
月度服务总结报告。

4.3.2.2.2自然资源云专区基础组件运行维护服务

4.3.2.2.2.1服务内容

对本项目运维的6个应用所涉及的各基础环境实例组件（如操作系统、OBS、TKE、TSF等）开展集约化运行维护工作，高效保障基础环境稳定运行，确保底层资源的高可用性和性能，减少因软件漏洞、配置错误或网络故障导致的基础服务中断。同时，严格的基础环境权限管理、补丁更新和安全加固能够有效防御外部攻击和数据泄漏风险，为上层应用提供可靠、安全的支撑环境。本服务范围严格限定于基础环境组件层（操作系统、中间件、容器平台、微服务平台、存储、网络组件等）的运行维护、配置管理、安全加固、性能优化（底层组件层面）、备份恢复（配置及平台日志），不包含上层业务应用的功能、代码、业务配置、业务数据逻辑、业务日志以及应用系统内部用户权限的管理和维护。

4.3.2.2.2.1.1组件环境监控

对系统各类基础环境实例组件的资源使用量、使用率、负载、性能响应、IO等进行实时监控和告警处理，及时发现基础环境存在的异常，并对告警和异常现象进行分析与处理。实时监控与管理工作包括监控对象及指标梳理、监控告警策略制定与优化、监控接入实施与采集器维护、基础资源使用实时监控、告警分析与跟踪处置、告警误报漏报问题分析与解决。监控对象与指标严格限定于基础环境组件层级。基础环境组件监控的主要工作如下：

- 1、监控对象及指标梳理：根据组件基础环境的实际情况，梳理其所使用到的相关基础环境组件，如服务器数量、操作系统类型等情况，并结合不同的对象梳理相应的监控指标，明确对同步监控对象相关指标的告警规则设置，以实现多云专区基础运行环境的精确监控。
- 2、监控告警策略制定与优化：制定符合基础环境实际运行需求的监控告警策略和级别管理；根据系统业务情况及时调整告警策略，优化各监控指标触发告警的阈值，针对不合理、无效的告警现象，对相应的监控策略进行收敛和优化，确保在问题发生时，能够及时发出有效的预警，避免告警信息泛滥。
- 3、监控接入与维护：针对梳理的监控对象，进行监控采集器的部署安装、调试以及维护工作，确保采集器正常运行，及时传输监控数据。
- 4、日常监控：定期对服务器、中间件等基础环境组件核心指标进行监控检查，包括CPU使用率、内存使用率、磁盘空间等，一是检查其使用率增长趋势是否异常，二是触发告警时，需及时安排运维人员进行响应。
- 5、告警分析与跟踪处置：针对告警信息进行分析，排查告警信息的根因，解决引起告警的故障和问题，并对告警和解决情况进行详细记录；若一线运维人员无法解决时，需要及时上升二线技术专家处理；此外，需定期对监控数据进行收集、统计与分析，并针对分析结果提出相应的优化建议。

4.3.2.2.2.1.2例行巡检

对系统各类基础环境实例组件开展定期巡检，通过巡检及时了解基础环境运行的运行情况，从而降低基础环境故障发生率并提升响应和处理速度，巡检工作包括巡检指标及梳理、巡检计划制定与优化、巡检实施等内容。巡检指标严格限定于基础环境组件的健康度、资源状态和平台性能。具体巡检工作内容如下：

- 1、梳理巡检指标：针对涉及性能容量、可用性、可连续性等运维对象的巡检指标，形成云专区基础组件巡检清单，明确巡检指标的异常判断标准和依据、巡检操作等方法。关键巡检指标如下表：

表3-12 基础环境巡检指标项

资源类型	产品名称	核心巡检项
容器服务	TKE	Pod状态、资源使用率(CPU/内存)、资源分配率(CPU/内存)、存储卷状态、日志事件等
文件存储	NAS	挂载状态、存储使用率等
对象存储	OBS	访问状态、存储使用率等

- 2、巡检计划制定与优化：基于梳理好的巡检指标制定合理的巡检计划，明确基础环境巡检的范围、时间、频率、记录与改进等；同时，根据历史巡检数据和实际异常发生情况，持续优化巡检周期、指标，确保巡检工作的高效性与问题发现的及时性。

3、巡检实施：定期按照巡检计划对服务器、中间件等基础环境组件开展例行巡检工作，及时记录CPU、内存、存储等关键指标状态。

4、异常分析与跟踪处置：当巡检指标出现异常时，及时进行排查分析，分析异常出现的原因，并提供解决方案；若一线运维人员无法解决时，需要转二线技术专家升级处理，并做好处理进度跟踪工作。

5、巡检故障识别遗漏分析：通过监控告警、用户上报等途径收集巡检时未能识别的故障和问题，进行遗漏识别该故障问题的原因分析，并制定相应的问题解决预案。

6、巡检报告编写

根据巡检的结果输出相应巡检报告，记录基础环境相关指标项的运行情况、异常问题点等，并及时提交巡检报告。

4.3.2.2.1.3故障处理

提供对系统各类基础环境实例组件的故障处理服务，严格按照故障定级与流程开展故障处理工作，确保快速响应与恢复。针对操作系统故障，通过日志分析、驱动修复或系统文件替换等措施恢复运行，并完成基础服务稳定性验证；数据库故障处理针对数据库服务可用性恢复、存储层面数据完整性检查（非业务逻辑）及性能优化（数据库实例层面）；中间件故障通过日志诊断和中间件自身性能调优解决，并完成中间件服务验证；网络故障采用拓扑分析与抓包定位，快速隔离并修复异常。当故障现象涉及多个基础环境组件或外部系统接口调用时，主导或协调相关团队进行跨系统联合排查定位，分析接口调用链路上的性能瓶颈或配置问题（如网络连通性、防火墙策略、API网关状态、服务端点健康状态等），协同解决跨系统依赖导致的故障。同时，建立与云平台、基础环境运维、应用运维、开发等的协同机制，沟通故障对应用访问的可能影响范围，通过多方协力优先恢复基础服务。故障根因分析与优化建议聚焦于基础环境层。常见基础环境故障如下：

1、操作系统故障：通过排查系统内核参数配置不当、安全策略配置问题、驱动程序异常等问题，制定针对性方案，在非业务高峰期谨慎实施，完成后全面验证操作系统服务测试。

2、中间件问题解决：通过分析中间件的配置文件，检查各项配置参数是否符合业务需求和最佳实践。通过中间件的日志文件，深入了解其内部运行机制中出现的异常情况；制定针对性方案，在非业务高峰期谨慎实施，完成后全面验证中间件服务测试。

3、跨系统接口调用故障：通过分析网络日志（TCP握手、丢包、延迟）、中间件/API网关日志（连接状态、超时、错误码）、服务端点健康状态（容器/Pod状态、进程资源占用）等，定位接口调用链路上的故障点（如网络策略阻断、DNS解析失败、服务端点不可达或高负载、API网关配置错误、认证授权失败、异步配置、连接池配置等），协调相关团队进行修复。

4.3.2.2.1.4安全加固

对系统各类基础环境实例组件层级的安全风险进行加固，包括云平台监控等保测评、安服扫描等发现的基础环境系统实例组件安全风险进行整理分析，并及时对基础环境进行安全加固和漏洞修复。安全加固工作包括基础环境版本升级、基础环境安全基线加固等。根据风险等级（高/中/低危）制定分级修复计划，优先处理高危漏洞；同时，需要进行充分的测试验证（基础服务层面），避免影响正常业务开展；完成漏洞修复后，按需输出漏洞修复报告。基础环境安全加固主要工作如下：

1、基础环境版本升级：针对存在版本漏洞风险的操作系统、中间件以及数据库等进行版本升级等。版本升级优先通过官方补丁修复漏洞，针对无法直接升级的版或无法直接修复的漏洞，通过配置调整或第三方组件替换规避已知漏洞，降低漏洞风险。

2、基础环境安全基线加固：一是结合系统的实际安全需求，制定适合本系统的基础环境安全基线。对操作系统、数据库、中间件等基础环境的各项安全配置进行检查，包括但不限于账号密码策略、访问控制权限、安全服务启用状态等，针对不符合安全要求的配置项进行整改，确保安全基线的合理性、完整性和可操作性。二是定期对基础环境的安全配置进行复查，确保安全配置的持续性和有效性。对于发现的不符合安全基线的配置项，及时进行整改和修复。三是弱密码整改，明确密码设置规范和要求，定期进行系统弱密码排查，如果发现使用弱密码，及时提醒用户进行修改；新用户注册设置密码时，严格审核密码合规性，避免使用弱密码。四是网络策略收敛，按照网络安全管理策略，通过分析现有网络访问规则（如防火墙策略、安全组、ACL等），识别冗余、冲突或过宽的权限，逐步收敛至最小必要访问原则，降低网络攻击面，提升整体安全性。

4.3.2.2.1.5架构与性能优化

按需开展基础环境架构与性能优化服务，针对系统各类基础环境实例组件版本或配置进行升级优化，如操作系统、数据库、中间件等，提升底层的支撑能力。优化工作严格限定于基础环境层配置与参数。当上层应用性能问题可能涉及底层资源瓶颈或配置不当（如数据库连接池耗尽、网络带宽不足、磁盘IOPS低、操作系统内核参数限制等）时，提供基础环境层级的性能数据监控、日志分析支持，并协助应用团队进行跨系统调

用链路性能瓶颈排查。根据分析结果，在基础环境层实施相应的优化措施（如调整连接池大小、优化网络配置、升级硬件或存储性能、调整内核参数等）。主要优化工作如下：

1、容器优化：对容器集群的架构设计和资源配置进行全面梳理，明确集群部署是否存在单节点风险、Pod资源分配不均、负载均衡策略不合理等问题；针对性开展容器环境优化工作，如完善高可用部署方案、调整Pod资源配额和调度策略、优化网络配置（平台层网络，非业务路由）和存储性能等... 通过实施弹性扩缩容机制、（平台层）资源使用情况监控分析，精准定位基础环境资源瓶颈，实现容器服务的动态调优和性能提升。

2、操作系统优化：对操作系统的配置进行梳理，明确系统是否存在资源分配不合理、磁盘LVM混用、内核参数未优化、磁盘I/O性能低下等问题；针对性开展操作系统环境优化工作..... 同时，通过资源监控和性能分析，精准定位系统资源瓶颈，如调整内核关键参数、优化磁盘调度算法和文件系统配置、升级安全补丁和性能补丁等，提升操作系统的运行效率和稳定性。同时，通过资源监控和性能分析，精准定位系统瓶颈，结合服务进程管理和资源调度优化，实现操作系统性能的持续调优和可靠运行。

3、跨系统性能协助：提供实例组件环境（CPU、内存、磁盘IO、网络带宽）及关键服务（数据库、中间件）的性能监控数据与日志；协助分析基础环境资源瓶颈对上层应用性能的影响；参与跨系统调用链路性能问题联合排查，在实例组件层实施识别出的优化点（如数据库参数优化、中间件连接池调整、网络QoS配置、存储性能升级等）。

4.3.2.2.2.1.6备份管理与恢复

协助对系统各类基础环境实例组件的配置信息、相关重要日志（如操作系统日志、数据库错误日志、中间件访问日志等）等进行备份管理，避免因系统故障或者操作失误导致基础环境重要配置数据或日志信息丢失。备份管理工作包括备份对象梳理、备份策略制定、备份申请与接入、备份作业检查等。主要工作内容如下：

1、备份需求梳理：根据各基础环境的实际备份需求，梳理相应的备份对象，并对需要备份的对象建立台账，详细记录各对象的备份内容（如重要的环境配置文件：`/etc/ssh/sshd_config`、`//var/log/syslog`等）、备份方式、备份策略和验证周期。

2、备份策略制定：根据基础环境的连续性、系统实际运行情况及系统安全等级要求制定各备份对象相应的备份策略和恢复策略，明确备份任务的时间、频率、保存期限等，并且对制定好的备份策略进行评估，确定备份策略的可用性。

3、备份申请和接入：根据实际备份需求，进行备份服务接入，按既定的备份策略申请备份接入，接入过程中按相关引导实施备份接入工作，如安装agent、配置路由、修改数据库配置等。

4、备份作业检查：定期查看备份作业执行状态，关注任务失败或报错情况，分析错误日志，对备份失败的作业提交补备任务。

5、备份失败修复：每周针对备份失败的策略进行分析处理，重新安装agent，调整配置等。

6、备份恢复：当出现系统异常时，协调开展备份恢复工作，确保数据的完整性。

4.3.2.2.2.1.7重保服务

为确保关键业务系统在重大活动、重要时点期间的基础环境稳定运行，需组建专业基础环境重保团队，实施7×24小时全天候基础环境安全保障。重点强化基础环境的实时监控与防护，通过并发数限流、黑白名单（网络/平台层）等方式保障基础环境正常运行；建立分钟级响应机制，确保基础环境安全事件5分钟内发现、15分钟内上报、1小时内处置。重保团队每日提交基础环境安全态势报告，所有处置操作留痕审计，保障结束后输出总结报告并持续优化防护策略。重保团队核心职责为保障基础环境稳定，业务功能的连续性保障需应用团队共同参与。

4.3.2.2.2.1.8应急演练与处置

需配合开展基础环境应急演练和处置服务，提升基础环境突发事件应对能力。建立常态化基础环境应急演练与处置机制。重点包括：组建专业基础环境应急响应团队，制定覆盖基础环境系统宕机、平台服务中断等典型场景的处置预案，明确分级响应流程；建立事件快速通报机制，规范处置流程；定期开展实战化基础环境应急演练，重点检验基础环境安全事件处置、基础服务故障恢复等关键能力。此外，需建立演练评估机制，结合应急演练过程中暴露的问题，持续优化基础环境实例组件应急预案。

4.3.2.2.2.2服务成果

云专区基础组件运行维护服务月报（含本月运行情况概述、实时监控、定期巡检、告警处置、应急保障等服务内容总结）；服务期结束提供项目服务总结报告。

4.3.3其他运行维护服务

4.3.3.3广东省自然资源业务网（业务网平面）网络平面运维服务

4.3.3.3.1服务内容

服务内容包括为电子政务外网自然资源业务网平面提供网络巡检、配置变更、故障处理等。

4.3.3.3.1.1网络巡检服务

提供网络巡检服务，查看网络运行的健康状态、网络运行流量、告警等情况。

4.3.3.3.1.2配置变更服务

为专用业务网络平面提供配置变更服务，包括网络策略变更、路由配置变更等内容。

4.3.3.3.1.3故障处理服务

为专用业务网络平面提供故障处置服务，包括故障分析、故障处理等。

4.3.3.3.2服务成果

网络平面运维服务月报（含本月巡检、配置变更、故障处置等服务内容）。

5.服务要求

5.1技术要求

5.1.1基础设施服务

5.1.1.1专业基础设施服务

5.1.1.1.1可视化屏租赁服务

5.1.1.1.1.1服务要求

租赁期内提供设备维护服务，保证可视化屏及配套环境的稳定运行，维护工作包括季度巡检服务和故障处理服务两项。

定期巡检服务：以季度为单位，对可视化屏及配套环境进行季度巡检，定期监测硬件（软件）的健康运行状态，发现存在的隐患，及时更换相应的配件或升级系统，及时消除隐患。

故障处理服务：对于使用过程中出现的故障，按照服务响应的要求及时派员进行处置，使硬件（软件）恢复正常状态。如发生的故障，经确认更换配件无法满足的，应提供备件，备件功能、性能不得低于原有租赁的设备。

5.1.1.1.2安全和密码资源池租赁服务

5.1.1.1.2.1服务要求

租赁期内提供设备维护服务，保证安全和密码资源池的稳定运行，维护工作包括季度巡检服务和故障处理服务两项。

定期巡检服务：以季度为单位，对安全和密码资源池进行季度巡检，定期监测硬件（软件）的健康运行状态，发现存在的隐患，及时更换相应的配件或升级系统，及时消除隐患。

故障处理服务：对于使用过程中出现的故障，按照服务响应的要求及时派员进行处置，使硬件（软件）恢复正常状态。如发生的故障，经确认更换配件无法满足的，应提供备件，备件功能、性能不得低于原有租赁的设备。

防御能力测试服务：租赁期内对安全资源池开展一次防御能力测试，验证安全资源池的防御能力和威胁检测能力的有效性。

授权数量包干升级服务：考虑到专业基础设施服务为按照现有实际规模进行的采购，但实际运营工作过程中由于涉及到各类测试等需要授权等实际情况，为保障安全资源池资源能够足量提供，需要配置一定的冗余，本项工作采用包干的形式。

5.1.1.1.3全厅REDIS租赁服务

5.1.1.1.3.1服务要求

租赁期内提供在线分布式缓存能力，满足自然资源系统用户高并发及数据快速访问的业务诉求，以支撑大规模数据访问，对数据查询效率要求高，且数据结构简单，不涉及太多关联查询的场景对缓存数据库的需求；提供维护服务，包括月度巡检服务和故障处理服务两项。

定期巡检服务：以月度为单位，对REDIS数据库进行月度巡检，定期监测健康运行状态以及使用率，发现存在的隐患，及时升级或完善数据库，及时消除隐患。

故障处理服务：对于使用过程中出现的故障，按照服务响应的要求及时派员进行处置，使数据库系统恢复正常状态。

5.1.1.1.4 CA设备及证书租赁服务

5.1.1.1.4.1服务要求

- 1.在租赁期内，供应商应严格遵守《电子认证服务管理办法》《电子认证服务密码管理办法》要求，维护双方权益，保证采购人的认证服务安全使用。
- 2.供应商提供的证书须支持SM2国密算法和国密安全协议。
- 3.供应商必须提供以下认证服务的故障及维护服务：提供全年7*24小时的不间断故障申报服务，故障申报响应时间不超过30分钟，故障恢复时间不超过4小时。
- 4.供应商必须提供CA证书的申请、延期、更换服务，保障采购人用户证书的正常可用。
- 5.供应商提供的CA证书必须支持Windows、Linux、统信UOS等操作系统，并提供与操作系统匹配的驱动程序。

5.1.1.1.5安全产品特征库升级授权租赁服务

5.1.1.1.5.1服务要求

表3-1 安全产品服务要求

序号	产品（服务）名称	特征库技术（服务）要求	数量
1	网御星云Power V6000-F83 G2-HD万兆防火墙	一年入侵防御特征库升级服务（适用于Power V6000-F83G2-HD）。入侵防御特征库包括脆弱口令、缓冲溢出、信息窃取、安全扫描、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞等。	2台
2	网御星云Power V6000-F83 G2-HD万兆防火墙	一年防病毒特征库升级服务（适用于Power V6000-F83G2-HD）。支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略，防止病毒源主机访问内部网络，提高网络整体安全性。	2台
3	网御星云Power V6000-F731 0	一年入侵防御特征库升级服务（适用于Power V6000-F7310）。入侵防御特征库包括脆弱口令、缓冲溢出、信息窃取、安全扫描、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞等。	2台
4	网御星云Power V6000-F731 0	一年防病毒特征库升级服务（适用于Power V6000-F7310）。支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略，防止病毒源主机访问内部网络，提高网络整体安全性。	2台
5	网御星云Power V6000-F731 0	一年上网行为管理特征库升级服务（适用于Power V6000-F7310）。支持对P2P下载、视频软件、游戏软件、炒股软件等识别和管控。	2台
6	网御星云TD3000-GS3500	一年入侵检测特征库升级服务（适用于TD3000-GS3500）。可对间谍软件、木马后门、刺探扫描、暴力破解、拒绝服务、缓冲区溢出、欺骗劫持、僵尸网络、SQL注入、XSS、Xpath、网页木马、钓鱼网站、Webshell、数据库攻击、网络设备攻击、可疑行为等常见攻击具有高精度的检测能力。	1台
7	网御高级持续性威胁检测与管理系统	一年入侵检测特征库升级服务（适用于APT3000-TD-M）。可对间谍软件、木马后门、刺探扫描、暴力破解、拒绝服务、缓冲区溢出、欺骗劫持、僵尸网络、SQL注入、XSS、Xpath、网页木马、钓鱼网站、Webshell、数据库攻击、网络设备攻击、可疑行为等常见攻击具有高精度的检测能力。	1台

- 1.提供1年特征库升级服务；
- 2.维保期内，各安全产品的升级软件包，必须与现有安全产品无缝兼容；
- 3.维保期内，为用户提供必要的技术支持、技术咨询等服务。

5.1.1.1.6安全基础设施租赁服务

5.1.1.1.6.1服务要求

各项技术规格要求见下表。

防火墙技术规格要求：

表3-2 防火墙技术要求

序号	指标项	技术要求
1	硬件架构	标准机架式设备，实配双电源；
2	硬件能力	千兆电口≥4，千兆光口≥8，万兆光口≥6，光口配置多模模块；
3	性能要求	网络层吞吐量≥40Gbps，应用层检测吞吐量≥12Gbps；
4		每秒新建连接数≥25 万；
5		最大并发连接数≥1000万；
6	路由	支持静态路由、策略路由，OSFP、BGP、ISIS 等路由；
7	可靠性	支持双机热备，支持主主部署模式、主备部署模式；
8	入侵防御功能	支持防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等；
9		IPS特征规则库不少于30000条；
10	应用识别及控制	配置应用识别控制功能模块；模块应包括对 P2P，IM，网络游戏，炒股软件， 语音聊天工具，流媒体， 常用邮件以及远程控制软件等的识别和控制；
11	DDOS防护	支持 SYN Flood、SYN ACK、UDP Flood 等DDoS 防护，支持 HTTP Flood、HTTPS Flood 等应用层 DD oS 防护；
12	防病毒功能	▲具有自主知识产权的病毒防护引擎，具备3个或以上防病毒引擎，支持多病毒引擎检测病毒（恶意文件）、阻止病毒（恶意文件）；（需提供报告封面具有CMA或者CNAS机构标识的第三方检测（检验或鉴定）报告复印件。）
13		支持上亿数量级的变种病毒库；
14	虚拟防火墙	支持不少于4个的虚拟防火墙，各个虚拟防火墙之间完全隔离；
15		每个虚拟防火墙具备独立的路由表；
16		支持每个虚拟系统可自定义CPU资源、会话数、策略数、安全域数、资源NAT规则数、目的NAT规则数、IPS EC VPN隧道数、会话限制规则数、IPS资源、统一资源定位系统资源、网络日志、威胁日志等配额；
17		支持在虚防火墙内独立配置病毒防护、漏洞利用防护、间谍软件防护、统一资源定位系统过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本系统内产生的日志进行独立审计；
18	响应方式	支持日志告警、SNMP TRAP 告警、会话阻断、IP 隔离、抓包取证等多种响应方式；
19	升级	支持在线升级、离线升级多种升级方式；
20	集中管理及易用性	支持图形化界面的报文追踪诊断及 Ping 诊断、Tracert 诊断功能。
21		支持五元组丢包统计功能。
22	报表	支持安全威胁的分析报表，提供基于威胁趋势、排行等呈现方式，支持接口流量、应用流量的分析报表，支持按日、周、月导出报表。
23	售后与维保	提供一年入侵防御、防病毒、应用识别特征库升级服务和一年原厂维保；
24	产品资质	具备《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证》。

万兆防火墙技术规格要求：

表3-3 万兆防火墙技术要求

序号	指标项	技术要求
1	硬件架构	标准机架式设备，实配双电源；
2	硬件能力	千兆电口≥4，千兆光口≥8，万兆光口≥4，光口配置多模模块；
3	性能要求	网络层吞吐量≥25Gbps，应用层检测吞吐量≥10Gbps，
4		每秒新建连接数≥25 万；
5		并发连接数≥900 万；
6	路由	▲支持多路由，具体如下：支持基于应用类型、统一资源定位系统类型、文件类型的策略路由，以实现为不同应用、统一资源定位系统、文件智能选择网络链路；策略路由支持轮询、随机、哈希、优先级等多种负载均衡算法选择；（需提供报告封面具有 CMA 或者 CNAS 机构标识的第三方检测（检验或鉴定）报告复印件。）
7	可靠性	支持双机热备，支持主主部署模式、主备部署模式；
8	入侵防御功能	支持防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等；
9		IPS特征规则库不少于30000条；
10	应用识别及控制	配置应用识别控制功能模块；模块应包括对 P2P，IM，网络游戏，炒股软件， 语音聊天工具，流媒体， 常用邮件以及远程控制软件等的识别和控制；
11	DDOS防护	支持 SYN Flood、SYN ACK、UDP Flood 等DDoS 防护，支持 HTTP Flood、 HTTPS Flood 等应用层 DD oS 防护；
12	防病毒功能	支持对 SMTP、POP3.HTTP、FTP 协议实现病毒扫描检测；
13		支持上亿数量级的变种病毒库；
14	虚拟防火墙	支持不少于4个的虚拟防火墙，各个虚拟防火墙之间完全隔离；
15		每个虚拟防火墙具备独立的路由表；
16		支持每个虚拟系统可自定义CPU资源、会话数、策略数、安全域数、资源NAT规则数、目的NAT规则数、IPS EC VPN隧道数、会话限制规则数、IPS资源、统一资源定位系统资源、网络日志、威胁日志等配额；
17		支持在虚防火墙内独立配置病毒防护、漏洞利用防护、间谍软件防护、统一资源定位系统过滤、文件过滤、 内容过滤、邮件过滤、行为管控等安全功能，并可支持对本系统内产生的日志进行独立审计；
18	响应方式	支持日志告警、SNMP TRAP 告警、会话阻断、IP 隔离、抓包取证等多种响应方式；
19	升级	支持在线升级、离线升级多种升级方式；
20	集中管理及易用性	支持图形化界面的报文追踪诊断及 Ping 诊断、 Tracert 诊断功能；
21		支持五元组丢包统计功能；
22	报表	支持安全威胁的分析报表，提供基于威胁趋势、排行等呈现方式，支持接口流量、应用流量的分析报表，支 持按日、周、月导出报表；
23	售后与维保	提供一年入侵防御、防病毒、应用识别特征库升级服务和一年原厂维保；
24	产品资质	具备《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证》。

终端安全管理系统技术规格要求：

表3-4 终端安全管理系统技术要求

序号	指标项	技术要求
1	控制台操作系统适配	形态软硬一体或纯软件，支持通过中国信息安全测评中心安全可靠测评的64位图形界面操作系统部署，包括但不限于中标麒麟、银河麒麟、统信等操作系统；
2	客户端操作系统适配	支持多种操作系统，包括但不限于统信、中标麒麟、银河麒麟、深度等通过中国信息安全测评中心安全可靠测评的64位图形界面操作系统；
3		要求客户端对终端系统CPU占用低于2%，内存占用低于200M，终端软件不大于1M。内置客户端资源监控机制，保证终端业务正常运行；
4	准入控制功能	支持终端入网检测，未通过认证的计算机、未经允许占用网络IP地址的设备不能接入网络；
5	资产信息采集	支持采集终端系统基本信息，包括操作系统、硬件信息等；
6		支持监控系统软件卸载、系统服务、计划任务、账户信息、进程、自动启动项信息、数据库资产、Web资产、中间件等信息；
7		支持系统日志类信息的采集、进程创建事件监控、目录、文件审核监控、注册表读写、U盘插拔读写监控；
8		支持新产生网络连接、断开事件的监控、监控链接发起端和接收端以及链接时长；
9		支持用户根据实际需求配置采集策略，包括定义采集周期和采集内容；
10	补丁管理	能够展示全网终端补丁的修复情况，能够完成从补丁下载、扫描、修复的全自动化后台操作；
11	外联管理	监控或阻止终端计算机通过WIFI、蓝牙等无线方式连接外部网络，杜绝违规外联行为，减少局域网安全隐患。同时，支持后台探测是否发生了两种或两种以上的网络连接行为；
12	外部设备管理	禁止终端计算机使用U盘、光驱、红外、蓝牙、MODEM、声卡、COM口，禁用图形图像设备，禁用便携式设备，禁用无线网卡；
13	威胁检测	支持内置轻量级病毒检测引擎，提供最新的热门和易攻击的病毒特征，方便快速查杀电脑关键位置及运行中的文件进程。
14		支持内置终端攻击事件分析能力，能够识别威胁事件，包括：APT攻击、勒索病毒、挖矿、蠕虫木马、感染型病毒、恶意程序、黑客程序、钓鱼、漏洞利用程序、黑名单进程等
15		支持通过对用户进程行为进行实时监控，结合父子进程链及进程通信行为分析，从攻击本质特征入手及时发现反弹Shell行为，并在告警中详细展示进程树及远控ip等信息。目前已识别支持的类型包括：bash反弹、c统一资源定位系统、wget、netcat各类命令反弹、脚本反弹、应用服务反弹等；
16	授权	提供不少于200个点的终端接入管理；
17	售后与维保	提供一年特征库升级服务和一年原厂维保；
18	产品资质	具备《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证》。

5.1.2运行维护服务

5.1.2.1基础设施运行维护服务

5.1.2.1.1基础设施运维服务

5.1.2.1.1.1服务要求

- 1.本项目基础设施运维服务将投入1名驻场运维人员（纳入本单位进行考勤）。
- 2.服务方需每月提供相关运维报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

服务方式包括：热线电话服务、远程服务和现场服务等。

对于基础设施运行维护，提供5×8小时现场和7×24小时热线电话两种运维服务；出现故障时快速响应，响应时间< 30分钟，安排运维人员处理；对需要返厂或送外维修的设备，要求提供备件替代直到原设备维修完成。重大故障提供故障分析报告。

5.1.2.2软件系统运行维护服务

5.1.2.2.1业务系统运行维护服务

5.1.2.2.1.1广东省自然资源一体化数据库（自然资源三维时空数据库）运行维护服务

5.1.2.2.1.1.1时空数据管理与服务

5.1.2.2.1.1.1.1服务要求

1.本项目软件系统运行维护服务将投入9名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.1.2时空图谱管理与服务

5.1.2.2.1.1.2.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.1.3影像智能识别管理与服务子系统（含遥感影像智能识别基础框架）

5.1.2.2.1.1.3.1服务要求

1.本项目软件系统运行维护服务将投入4名运维人员（由服务提供商进行考勤）。

2.每月提供相关运维报告至业主方相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护服务提供5×8小时远程或现场和7×24小时热线电话两种运维服务，及时响应业主需求，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2广东省自然资源一体化管理与服务平台（国土空间基础信息平台）运行维护服务

5.1.2.2.1.2.1广东省自然资源决策参阅子系统

5.1.2.2.1.2.1.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.2赋能中心(技术核查工具)

5.1.2.2.1.2.2.1服务要求

1.本项目软件系统运行维护服务将投入2名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.3赋能中心(资讯网)

5.1.2.2.1.2.3.1服务要求

1.本项目软件系统运行维护服务将投入2名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.4赋能中心(公众服务窗口、一体化审批)

5.1.2.2.1.2.4.1一体化审批平台运维服务

5.1.2.2.1.2.4.1.1服务要求

1.本项目软件系统运行维护服务将投入2名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.4.2公众统一服务窗口运维服务

5.1.2.2.1.2.4.2.1服务要求

1.本项目软件系统运行维护服务将投入2名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.5赋能中心(用户中心、消息中心、集成门户、数字政府公共能力中心)

5.1.2.2.1.2.5.1服务要求

1.本项目软件系统运行维护服务将投入4名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.6赋能中心(信息资源管理中心)

5.1.2.2.1.2.6.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.7业务能力中心(审批监管能力中心、调查监测能力中心、评价评估能力中心、预测预警能力中心)

5.1.2.2.1.2.7.1服务要求

1.本项目软件系统运行维护服务将投入4名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.2.8广东省自然资源一体化管理与服务平台（国土空间基础信息平台）-云GIS模块运维服务

5.1.2.2.1.2.8.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤），以线上线下相结合的方式提供维护服务。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.3广东省自然资源和不动产登记综合应用运行维护服务

5.1.2.2.1.3.1广东省不动产登记综合应用（省级端）

5.1.2.2.1.3.1.1服务要求

1.本项目软件系统运行维护服务将投入5名运维人员（由服务提供商进行考勤）。

2.每周、每月提供相关运维报告至业主方相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 运维服务指标要求

运维质量方面，需确保项目系统变更条件准备充分，制定完整回退方案，避免出现系统故障或安全事故，尤其是人为因素造成的系统故障或者安全事故。

运维服务人员方面，需提供长期稳定的运维服务人员，并保障人员出勤率，建立维护日常沟通机制，确保沟通有效和及时。

5.1.2.2.1.3.2广东省不动产登记综合应用（市县端）

5.1.2.2.1.3.2.1服务要求

1.本项目软件系统运行维护服务将投入5名运维人员（由服务提供商进行考勤）。

2.每周、每月提供相关运维报告至业主方相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护服务提供5×8小时远程和7×24小时热线电话两种运维服务，及时响应业主需求，按时按量按要求提交相关材料，出现故障时，快速受理服务请求，业务系统根据不同的故障等级在不同时间内进行响应，出现故障时快速响应，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

2) 运维服务指标要求

运维质量方面，需确保项目系统变更条件准备充分，制定完整回退方案，避免出现系统故障或安全事故，尤其是人为因素造成的系统故障或者安全事故。

运维服务人员方面，需提供长期稳定的运维服务人员，并保障人员出勤率，建立维护日常沟通机制，确保沟通有效和及时。

5.1.2.2.1.3.3广东省不动产登记综合应用（公众侧）

5.1.2.2.1.3.3.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤）。

2.每周、每月提供相关运维报告至业主方相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护服务提供5×8小时远程和7×24小时热线电话两种运维服务，及时响应业主需求，按时按量按要求提交相关材料，出现故障时，快速受理服务请求，业务系统根据不同的故障等级在不同时间内进行响应，出现故障时快速响应，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

2) 运维服务指标要求

运维质量方面，需确保项目系统变更条件准备充分，制定完整回退方案，避免出现系统故障或安全事故，尤其是人为因素造成的系统故障或者安全事故。

运维服务人员方面，需提供长期稳定的运维服务人员，并保障人员出勤率，建立维护日常沟通机制，确保沟通有效和及时。

5.1.2.2.1.4广东省国土空间用途管制综合应用运行维护服务

5.1.2.2.1.4.1服务要求

本项目软件系统运行维护服务将投入6名运维人员（非驻场人员由服务提供商进行考勤，其中至少1名驻场，驻场人员纳入本单位进行考勤）。运维工程师需具备相关专业背景和丰富的运维经验，能够熟练掌握系统的各项功能和运维技术。

服务方需每月提供相关巡检报告至本项目相关负责人。运维报告内容可包括系统运行状态、故障处理情况、巡检结果、安全加固情况、用户支持情况等。运维报告应详细、准确、规范，能够全面反映系统的运维情况和存在的问题。

运维服务时限、指标要求：

1) 服务方式要求：

热线电话服务、远程服务和现场服务等。

2) 运维服务时限要求：

提供5×8远程服务和7×24小时热线电话两种运维服务，出现故障时，快速响应并受理服务请求，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

5.1.2.2.1.5广东省自然资源市场与资产监管综合应用运行维护服务

5.1.2.2.1.5.1广东省自然资源市场与开发利用监测监管子系统运行维护服务

5.1.2.2.1.5.1.1服务要求

本项目软件系统运行维护服务将投入8名运维人员（其中3人需驻场，纳入本单位进行考勤，非驻场人员由服务提供商进行考勤）。服务方需每月提供相关巡检报告至本项目相关负责人。

运维服务时限、指标要求：

1) 运维服务时限要求

本项目软件系统运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间，对上级主管部门要求开展重点保障工作的任务，需提供专业技术人员，配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤2 小时。

5.1.2.2.1.5.2广东省全民所有自然资源资产信息管理与监管子系统运行维护服务

5.1.2.2.1.5.2.1全民所有自然资源资产变更清查辅助模块

5.1.2.2.1.5.2.1.1服务要求

本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤）。

每周、每月提供相关运维报告至业主方相关负责人。

运维服务时限、指标要求：

1、运维服务时限要求

本项目软件系统运行维护服务提供7×24小时热线电话和线上运维服务，及时响应业主需求，按时按量按要求提交相关材料。出现故障时，快速受理服务请求，业务系统根据不同的故障等级在不同时间内进行响应，出现故障时快速响应，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

2、运维服务指标要求

运维质量方面，需确保项目系统变更条件准备充分，制定完整回退方案，避免出现系统故障或安全事故，尤其是人为因素造成的系统故障或者安全事故。

运维服务人员方面，需提供长期稳定的运维服务人员，并保障人员出勤率，建立维护日常沟通机制，确保沟通有效和及时。

5.1.2.2.1.5.2.2全民所有自然资源资产变更清查成果质量检查模块

5.1.2.2.1.5.2.2.1服务要求

本项目软件系统运行维护服务将投入3名运维人员（由服务提供商进行考勤）。

每周、每月提供相关运维报告至业主方相关负责人。

运维服务时限、指标要求：

1、运维服务时限要求

本项目软件系统运行维护服务提供7×24小时热线电话和线上运维服务，及时响应业主需求，按时按量按要求提交相关材料。出现故障时，快速受理服务请求，业务系统根据不同的故障等级在不同时间内进行响应，出现故障时快速响应，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

2、运维服务指标要求

运维质量方面，需确保项目系统变更条件准备充分，制定完整回退方案，避免出现系统故障或安全事故，尤其是人为因素造成的系统故障或者安全事故。

运维服务人员方面，需提供长期稳定的运维服务人员，并保障人员出勤率，建立维护日常沟通机制，确保沟通有效和及时。

5.1.2.2.1.5.2.3全民所有自然资源资产信息管理监管模块

5.1.2.2.1.5.2.3.1服务要求

本项目软件系统运行维护服务将投入8名运维人员（其中2人需驻场，纳入本单位进行考勤，非驻场人员由服务提供商进行考勤）。

每周、每月提供相关运维报告至业主方相关负责人。

运维服务时限、指标要求：

1）运维服务时限要求

本项目软件系统运行维护服务提供5×8小时远程和7×24小时热线电话两种运维服务，及时响应业主需求，按时按量按要求提交相关材料，出现故障时，快速受理服务请求，业务系统根据不同的故障等级在不同时间内进行响应，出现故障时快速响应，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

2）运维服务指标要求

运维质量方面，需确保项目系统变更条件准备充分，制定完整回退方案，避免出现系统故障或安全事故，尤其是人为因素造成的系统故障或者安全事故。

运维服务人员方面，需提供长期稳定的运维服务人员，并保障人员出勤率，建立维护日常沟通机制，确保沟通有效和及时。

5.1.2.2.1.6广东省测绘地理信息管理综合应用运行维护服务

5.1.2.2.1.6.1广东省测绘地理信息监管与服务系统运行维护服务

5.1.2.2.1.6.1.1服务要求

1.本项目软件系统运行维护服务将投入4名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1）服务方式要求：

热线电话服务、远程服务、邮件服务和上门故障处理服务等。

2) 运维服务时限要求:

提供5×8远程服务和7×24小时热线电话两种运维服务,出现故障时,快速响应并受理服务请求,根据系统等级和故障等级划分标准进行响应,对于远程或电话无法解决的问题,安排技术人员现场处理,重大故障提供故障分析报告。

5.1.2.2.1.6.2天地图·广东子系统运行维护服务

5.1.2.2.1.6.2.1服务要求

1.本项目软件系统运行维护服务将投入2名运维人员(由服务提供商进行考勤)。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求:

1) 运维服务时限要求

本项目软件系统运行维护,提供7×24小时热线电话服务,出现故障时快速响应,业务系统运行维护响应时间<30分钟;判断故障是否能远程解决,能远程解决的故障,应接到维护需求后30分钟内进行远程协助故障处理;对于远程无法解决的问题,安排技术人员2小时内到达现场进行处理,重大故障提供故障分析报告。

2) 重保服务要求

在国家重大活动和重大突发事件期间,对上级主管部门要求开展重点保障工作的任务,需提供专业技术人员,配合开展本项目软件系统的重保工作。工作内容包括但不限于系统状态监控、安全漏洞排查与修复、应急响应、定时更新汇报等。

3) 系统稳定性要求

系统应保证7*24小时不间断运行;做好数据备份和恢复,在系统出现紧急情况时,修复时间MTTR≤2 小时。

5.1.2.2.1.6.3广东省遥感影像管理与服务子系统(卫星遥感影像管理与服务)运行维护服务

5.1.2.2.1.6.3.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员(其中3人均需驻场,纳入本单位进行考勤)。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求:

1) 服务方式要求:

热线电话服务、远程服务和现场服务等。

2) 运维服务时限要求:

提供5×8远程服务和7×24小时热线电话两种运维服务,出现故障时,快速响应并受理服务请求,根据系统等级和故障等级划分标准进行响应,对于远程或电话无法解决的问题,安排技术人员现场处理,重大故障提供故障分析报告。

5.1.2.2.1.7广东省自然资源厅城市地质信息管理服务平台运行维护服务

5.1.2.2.1.7.1服务要求

1.本项目软件系统运行维护服务将投入3名运维人员(由服务提供商进行考勤)。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求:

1) 服务方式要求:

热线电话服务、远程服务和现场服务等。

2) 运维服务时限要求:

提供5×8远程服务和7×24小时热线电话两种运维服务,出现故障时,快速响应并受理服务请求,根据系统等级和故障等级划分标准进行响应,对于远程或电话无法解决的问题,安排技术人员现场处理,重大故障提供故障分析报告。

5.1.2.2.1.8广东省国土资源技术中心政务服务综合保障子系统运行维护服务

5.1.2.2.1.8.1服务要求

1.本项目软件系统运行维护服务将投入2名运维人员(由服务提供商进行考勤)。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 服务方式要求：

热线电话服务、远程服务和现场服务等。

2) 运维服务时限要求：

提供5×8远程服务和7×24小时热线电话两种运维服务，出现故障时，快速响应并受理服务请求，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

5.1.2.2.2业务系统支撑环境运行维护服务

5.1.2.2.2.1自然资源云专区数据库实例运维服务

5.1.2.2.2.1.1服务要求

1.本项目数据库运行维护服务将投入6名数据库工程师（由服务提供商进行考勤）。

2.服务方需每月提供运维服务月报至本项目相关负责人。

3.运维服务时限、指标要求：

1) 服务方式要求：

热线电话服务、远程服务和现场服务等。

2) 运维服务时限要求：

提供5×8远程服务和7×24小时热线电话两种运维服务，出现故障时，快速响应并受理服务请求，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

5.1.2.2.2.2自然资源云专区基础组件运行维护服务

5.1.2.2.2.2.1服务要求

1.本项目基础环境运行维护服务将投入7名运维人员（由服务提供商进行考勤）。

2.服务方需每月提供相关巡检报告至本项目相关负责人。

3.运维服务时限、指标要求：

1) 运维服务时限要求

本项目基础环境运行维护，提供7×24小时热线电话服务，出现故障时快速响应，业务系统运行维护响应时间<30分钟；判断故障是否能远程解决，能远程解决的故障，应接到维护需求后30分钟内进行远程协助故障处理；对于远程无法解决的问题，安排技术人员2小时内到达现场进行处理，重大故障提供故障分析报告。

2) 基础环境稳定性要求

基础环境应保证7*24小时不间断运行；做好数据备份和恢复，在系统出现紧急情况时，修复时间MTTR≤4 小时。

5.1.2.2.3软件系统运行维护服务其他要求

5.1.2.2.3.1云资源与权限管理

1.在采购人组织与授权下，与政务云服务提供方紧密协作，开展云资源台账维护、权限管理、负载监控、网络策略管控、应急响应及全链路故障排查；协助完成网络安全等级保护测评和商用密码应用安全性评估；妥善使用采购人授权的网络安全权限，保障系统稳定与数据安全。

2.按照采购人规划的云资源管理权限要求，规范执行堡垒机和VPN账号的操作。

3.基于性能测试数据，按照政务云管理要求编制云资源测试报告，作为资源申请要件。

5.1.2.2.3.2系统部署与运行环境构建

1.负责云资源管理、系统运行环境构建与配置，在部署阶段同步落实监控、日志采集、安全策略和备份恢复机制，确保系统具备高可用性、可观测性和安全性；系统上线后，须提供性能优化、故障响应、系统变更管理、例行巡检、问题分析与改进等全周期运维保障服务。

2.如有系统升级迭代部署要求，需遵循政务云原生技术架构与最佳实践，编制系统部署方案，为部署工作提供清晰、具体、可操作的指导。

3.根据部署方案完成运行环境构建，包括：根据互访、对接及监控需求提出网络策略开通申请；依据性能基线与安全基线完成操作系统初始化；部署应用系统所需基础软件。

4.协助实施系统初始化中的数据迁移工作；负责联调迭代过程中的运行环境加固；完成迭代联调后，须提出上线安全风险评估需求（含网络

策略申请），并协同承建方根据测评结果进行安全整改。

5.1.2.2.3.3运维保障与安全管控

1.按巡检计划明确具体责任人，对政务云存储、计算资源、中间件、数据库、系统日志、备份及安全策略等进行全面检查，及时记录并报告问题与隐患。

2.当作为变更实施方或提出方时，须对已交付系统变更提交包含变更目标、时间计划、影响范围、风险评估及应对措施、变更步骤与回退步骤的详细方案；变更实施过程中须通报进展，配合业务验证。

3.在系统变更完成后，及时更新运维手册、部署手册、使用手册、三方测试方案、系统拓扑图、资源配置表等运维技术档案，保证配置信息的完整性与准确性。

4.配合采购人，定期参与对现有运维和故障处置流程的评估，查找流程运行不畅环节，提出改进建议。

5.定期对系统运行状态的监控数据和日志数据进行比对分析，识别潜在隐患和系统运行瓶颈，为运维质量管理和云资源动态管控提供数据指标支撑。

6.配合采购人组织的定期风险评估，参与识别可能引发故障的关键因素（如云资源故障隐患、软件缺陷、人为错误或自然灾害等），协助确定重点防范环节并制定相应预防措施。

7.配合采购人持续完善系统运行状态监控机制，根据要求应用自动化监控技术，对所管理的信息系统实施持续、常态化监控；定期配合评审预防措施的有效性，协助更新和维护应急策略。

8.配合采购人结合信息系统特点和业务需求制定应急预案（涵盖云资源故障、应用系统故障、安全攻击等），明确各类故障的应急处理步骤、报告请示程序和应急联络名单；定期参与应急演练，模拟不同类型故障事件，检验预案有效性和可操作性，确保相关人员熟悉预案内容与操作流程。

5.1.2.2.3.4故障与应急管理

1.配合故障分级通报要求，协同采购人对系统故障关联方进行通报。

2.故障处理遵循“先抢通、后修复”原则，须安排专人记录故障具体情况，参与故障初步识别与分类，进行深入故障分析并制定处置方案。

5.1.2.2.3.5运维标准化与人员能力

1.配合采购人不定期修订完善标准化运维流程和操作指南，提供具体技术支撑，确保运维操作有明确的操作规范可依。

2.定期对运维人员技能进行考核评估，确保人员能力有效胜任岗位工作，考核评估结果应可供采购人查验。

5.1.2.3其他运行维护服务

5.1.2.3.1广东省自然资源业务网（业务网平面）网络平面运维服务

5.1.2.3.1.1服务要求

1.本项目软件系统运行维护服务将投入1名运维工程师（由服务提供商进行考勤）。

2.服务方需每月提供运维服务月报至本项目相关负责人。

3.运维服务时限、指标要求：

1）服务方式要求：

热线电话服务、远程服务和现场服务等。

2）运维服务时限要求：

提供5×8远程服务和7×24小时热线电话两种运维服务，出现故障时，快速响应并受理服务请求，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告。

5.2项目质量管理要求

5.2.1服务团队岗位职责清单

详见5.3.1服务人员。

5.3管理要求

5.3.1服务人员

★服务商应指派固定的团队为本项目提供专业服务，服务团队成员不得少于113人，人员不得复用。（提供承诺或声明，格式自拟）。

序号	成员 角色	职责	资历及资质要求	数量	是否要求驻 场	备注
1	项目负责人	整体负责项目的统筹管理，负责运维工作的规划与管理。	具有计算机类专业本科或以上学历 2、具有系统规划与管理师证书或信息系统项目管理师（计算机技术与软件专业技术资格） 3、作为项目负责人（项目经理）具有运维相关项目管理经验	1	/	如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。
2	软件系统运维（安全）负责人	整体负责项目信息系统的安全制度构建、系统安全维护及系统安全审计，保障信息系统运维过程中的安全。	1、具有信息安全相关专业本科或以上学历 2、具有信息安全工程师证书（计算机技术与软件专业技术资格） 3、作为运维安全负责人具有安全运维相关项目管理经验	1	/	如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。
3	软件系统运维（各业务子系统运维）负责人	1. 负责各业务子系统的具体系统的运维规划与管理工作； 2. 分析用户运维需求，了解系统开发标准和架构，能及时分析系统出现的故障并提出解决方案； 3. 从事信息系统一线运维实施等日常运维管理工作。	1、具有计算机类或信息系统类或电子信息类本科或以上学历 2、具有系统规划与管理师或系统分析师或系统集成项目管理工程师（计算机技术与软件专业技术资格） 3、具有信息系统运维相关项目经验	19		如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。

4	软件系统运维（各业务子系统运维）工程师	负责各业务子系统的具体运维工作	1、信息化工作经验	77	9人驻场： 广东省国土空间用途管制综合应用-1人； 广东省自然资源市场与开发利用监测监管子系统-3人； 全民所有自然资源资产信息管理监管模块-2人； 广东省遥感影像管理与服务子系统（卫星遥感影像管理与服务）-3人	
5	软件系统运维（业务系统支撑环境运维）负责人	负责软件系统运维（业务系统支撑环境运维）的日常统筹和管理工作。	1、具有计算机类专业本科或以上学历； 2、具有系统集成项目管理工程师（计算机技术与软件专业技术资格）； 3、具有业务系统支撑环境（云平台）相关项目经验	1	/	如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。
6	软件系统运维（业务系统支撑环境运维）云专区数据库运维工程师	负责软件系统运维（业务系统支撑环境运维）自然资源云专区数据库实例运维工作	1、具有计算机类专业本科或以上学历 2、具有数据库系统工程师证书（计算机技术与软件专业技术资格） 3、具有系统运维或数据库相关项目经验	6	/	如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。

7	软件系统运维（业务系统支撑环境运维）云专区基础组件运维工程师	1.掌握云专区硬软件与网络基本情况，基于信息系统运维需要和故障暴露的问题，完善云专区基础设施和网络架构； 2.实施自然资源云专区基础组件运维工作	1、具有计算机类或电子信息类专业本科或以上学历 2、具有系统架构设计师或网络工程师证书（计算机技术与软件专业技术资格） 3、具有云平台相关项目经验	6	/	如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。
8	业务网络平面运维和基础设施运维工程师	从事网络和基础设施运维工作。	1、具有网络工程相关专业本科或以上学历的 2、具有网络工程师证书（计算机技术与软件专业技术资格） 3、具有网络运维或基础设施运维相关项目经验	2	基础设施运行维护需1人驻场	如项目涉及分包，该处人员必须由主体投标方（即非分包承接商）的人员担任。
				113		

1.★投标人须整体承诺：投标文件所列全部拟投入人员，均视为项目实施实际投入人员；拟派驻现场的项目负责人、运维安全负责人、软件系统运维及各业务子系统运维负责人、软件系统运维（业务系统支撑环境运维）负责人等主要管理人员，须为本单位在职正式员工。投标人应自行拟定承诺函（函中需明确标注各人员对应岗位，明确固化拟投入人员即为项目实际实施人员），同时一并提交佐证材料：上述现场主要管理人员的劳动合同复印件，或投标截止日期前三个月内任意一个月的社保缴纳证明材料。

- 2.投标人须根据以上表格分项列出拟投入人员名单及资历情况。
- 3.投标人采取分包的，接受分包供应商应具备承接相关服务所需的专业服务人员并按招标文件提供人员资料。
- 4.投标人须书面承诺，如在项目实际执行过程中发生项目负责人不能按采购文件要求胜任相关工作的，采购人有权要求更换项目负责人，投标人必须在两周内调整为符合采购文件要求且能胜任相关工作的项目负责人并到位开展工作，否则采购人有权终止合同并报相关管理部门进行处理。
- 5.投标人承诺的项目负责人未经用户同意不得调整；投标人如中途更换项目负责人，应征得用户同意，否则采购人有权终止合同。
- 6.如需调整服务团队成员，须书面向采购人提出申请，说明申请理由，经采购人书面同意方可调整团队人员，调入人员的资历和从业经验不低于调出人员，否则视为违约行为，采购人有权终止服务合同。
- 7.应提供以上人员相关证明资料复印件并加盖公章，并提供以上人员在本公司任职的有效外部证明材料（如加盖政府有关部门印章的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，事业法人的相关人员应提供该单位的相关证明）复印件。
- 8.服务期间，投标人应配合采购人开展运维人员的考勤、离职、离岗等管理工作。

5.3.2进度要求

1.实施进度

本项目里程碑计划如下：

阶段	工作内容	里程碑事件/成果	时间
项目启动	建立项目团队与服务计划	项目启动会	合同签订后一个月内
项目方案设计	深入分析项目需求，制定并实施解决方案	项目总体服务方案	合同签订后一个月内
项目实施	基础设施服务、软件开发服务、运行维护服务	按服务要求提供	按服务期限执行
项目阶段性考核1	根据服务内容，对合同签订之日起至2026年10月的项目实施成果进行阶段性考核	按服务要求提供/考核评价表	2026年11月10日前
项目阶段性考核2	根据服务内容，对2026年11月至2027年2月的项目实施成果进行阶段性考核	按服务要求提供/考核评价表	2027年3月31日前
项目阶段性考核3	根据服务内容，对2027年3月至2027年5月的项目实施成果进行阶段性考核	按服务要求提供/考核评价表	2027年6月30日前
项目验收	确保交付物符合需求，完成验收流程	项目验收材料	按验收期限及成果交付期限执行

2.验收期限

项目服务期满之日起30个工作日内完成验收。验收前10个工作日，按采购人要求提交本项目验收前置审核有关成果资料。

3.成果交付期限

本项目通过验收之日起10个工作日内。

5.3.3组织实施要求

为使项目按质、按量、按时及有序实施，投标人应建立完善、稳定的项目团队、内部组织管理方式及管理机构、协调机制、技术基础，支撑保障要求及其他相关要求。在机制保障方面，成立组织实施小组和项目专家组的双轨制的组织模式。在项目日常管理和条件保障方面，从行政组织、后勤保障和支撑条件各方面创造良好的服务环境，确保项目的顺利实施。

5.3.4文档管理要求

投标人应在项目完成时，将本项目所有文档、资料汇集成册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，投标人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少3套，电子文档1套。以及应标文件（供应商盖章后的pdf电子版）。文档成果包括但不限于：

- 1.项目管理文档成果：项目总体服务方案；项目服务总结报告。
- 2.基础设施服务、软件开发服务、运行维护服务的文档成果详见“4服务内容”章节关于服务成果和交付物的要求。
- 3.其他文档成果：其他过程文档（如巡检记录、工单记录、故障处理报告等，如有发生）。

5.4验收标准

1.验收标准和条件

- （1）符合本项目采购文件中采购需求描述相关技术要求和中标人投标文件中承诺的相应技术指标或标准。
- （2）采购人与中标人在项目实施过程中约定的其他相关技术要求。

2.验收方式

由采购人组织专家进行验收，必要时，可邀请第三方机构进行验收。

5.5其他要求

5.5.1服务响应要求

在服务有效期内，投标人需配备专业专职技术服务队伍，及时响应采购人的服务要求，在经双方确认的约定工作量范围内提供技术支持和服务，包括但不限于以下内容：

(1) 服务响应可通过现场、远程等方式提供，由此产生的一切费用均由投标人承担。

(2) 对于基础设施服务：对本项目所租赁的专业基础设施服务提供必要的安装调试、备件更换、故障及维护服务。提供全年7*24小时的不间断故障申报服务，全年各类设施服务可用率为99.8%以上；如出现故障不能及时修复的，供应商要立即进行更换，故障修复后提交处理工单或报告。

(3) 对于硬件基础设施运行维护，提供5×8小时现场和7×24小时热线电话两种运维服务；对于软件系统运行维护和自然资源业务网络平面运维，提供5×8小时远程和7×24小时热线电话两种运维服务，出现故障时，快速受理服务请求，响应时间<30分钟。业务系统根据不同的故障等级在不同时间内进行响应，出现故障时快速响应，根据系统等级和故障等级划分标准进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理。

若上述内容与技术要求章节内容存在冲突，应以其中标准更严格的要求为准。

5.5.2资产权属

1.本项目不会引起任何已申请、登记的知识产权所有权的转移。

2.本项目所涉成品软件租赁服务成果的知识产权归属按下列第(3)种方式处理；本项目所涉基础设施租赁和运维服务成果的知识产权归属按下列第(4)种方式处理。

(1) 投标人负责开发软件服务，包括代码编写、调试、测试等开发工作，投标人为履行本项目义务所形成的服务成果的知识产权归采购人单独所有。

(2) 投标人负责提供定制软件租赁服务，采购人基于本合同约定委托投标人定制开发的产品、程序、服务等知识产权归甲、投标人共同所有，投标人应按采购人书面要求交付该共有部分的源代码；投标人在共有部分的基础上进行二次开发的及对二次开发形成的产品、程序等财产进行处置的，需经采购人书面同意，二次开发所形成的产品、程序、服务等知识产权归开发者所有，共有部分仍归甲、投标人共同所有。投标人根据采购人授权，利用项目成果申请的商标、专利或输出的图片、视频等受知识产权保护的成果物，采购人有权无条件永久使用。

(3) 投标人负责提供成品软件租赁服务，投标人为履行本合同义务所形成的所有服务成果的知识产权（除成品软件开发涉及的知识产权）归采购人单独所有。

(4) 本项目基础设施服务租用或运维服务，不涉及知识产权权属转移。

3.本项目所涉及的数据所有权归政府所有。投标人只能用于履行本项目之义务。

4.投标人提供的相关软件应是自行开发的产品或具备合法、合规授权，满足知识产权、安全等保三级等方面的有关规定和要求。

5.投标人保证向采购人提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因投标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，投标人应负责解决并赔偿因此给采购人造成的全部损失。

6.本项目所涉及的数据所有权归政府所有。数据资产的管理应遵循财政部《关于加强数据资产管理的指导意见》（财资〔2023〕141号）及其他相关法律、法规、政策要求。

5.5.3保密要求

1.投标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人工作秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

2.投标人不得以竞争为目的或出于私利或为第三人谋利而擅自保存、披露、使用采购人工作秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的工作秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的工作秘密和党政机关保密信息。投标人在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或投标人内部与该项目无关的任何人员。

3.投标人对于工作期间知悉采购人的工作秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。

4.严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

5.5.4监理要求

投标人须承诺，在项目开展过程中接受采购人指定的咨询监理机构的监理。

5.5.5考核评价要求

本项目分阶段对服务质量进行打分，并与款项支付挂钩。款项支付比例：

序号	评价分数范围	评价等级	支付比例
1	90分≤评价分数<100分	优秀	100%
2	75分≤评价分数<90分	良好	90%
3	60分≤评价分数<75分	中等	70%
4	评价分数<60分	一般	评价分数/100*100%

序号	考核方向	指标项	考核要点	得分
1	效率 (45)	服务响应及时率（10）	服务响应超过2小时，扣1分；超过4小时扣2分；超过6小时或以上，扣5分；超过24小时或以上，此项得零分并进行整改。	
2		阶段交付物提交及时性（10）	阶段交付物是否按照要求时间点提交，包含不限于项目实施过程提交的交付物文档。提交文件每延迟一天扣1分。	
3		故障到场及时率（10）	考核到场时间。如下规定时间内到达现场，每超出1小时扣5分（不足1小时按1小时计算，客观天气、交通因素除外）。（地级市区到达时间8小时内；有直达班车的县到达时间12小时内；无直达班车的县到达时间24小时内）	
4		故障处理及时率（15）	故障处理时间超过2天的，每次扣1分；故障处理时长超过4天的，每次扣2分；故障处理时长超过6天的，每次扣5分。	
5	质量 (25)	变更质量（5）	考核变更条件是否准备充分，是否造成故障，是否有完整回退方案，重大变更是否有准备并落实人员保障方案。每变更失败一次，扣1分。	
6		质量事故（10）	每发生一单人为事故，引起整个业务系统不可用，扣10分；关键业务功能受损或无法响应，但通过人为干预或规避可以在有限的时间内运行，扣8分；其他故障情况，扣3分；情节严重的，采购人有权追究法律责任，并终止项目。	
7		安全事故（10）	考核是否有因服务人员原因导致的人员事故、财产安全事故、信息泄露等安全事故。每发生一单人为事故，扣3分；情节严重的，甲方有权追究法律责任，并终止项目。	
8	管理	人员稳定性（10）	考核是否提供稳定的服务能力。 1.未按规定流程申请换人； 2.人员替换未做好交接工作（至少预留5个工作日交接时间，从人员申请更换被项目组批准后起算），对项目造成影响； 3.人员离职未能在10个工作日内补充合格的替代人员，从该人员离职申请得到项目组的批准后起算10个工作日； 4.同一项目在三个月内，换人次达到三次以上的； 以上满足任何1条则算作一次负向事件，扣2分。	

9	(30)	客户投诉（10）	是否与业主方保持通畅沟通，并积极响应工作要求等，投诉的内容包括但不限于人员素质、态度、违规、能力、工作质量、工作进度等。直接客户提出的有效投诉。每有效投诉1次，扣5分。	
10		人员出勤率（4）	排班要求人员每无故缺勤1次，扣1分。	
11		流程遵循（4）	考核人员是否遵守服务规范、项目实施规范、现场管理规范、机房管理规范、重大操作流程规范等。不论是否造成实质性的问题或者影响，经证实的违规行为，每违规1人次，扣1分。	
12		沟通机制（2）	考核日常沟通机制的及时性，包括但不限于周报、临时性汇报，可由维护主管根据实际情况调整。未及时汇报或隐瞒重要风险点1次，扣1分。	
合计				
考核人（甲方）签名：被考核人（乙方）签名：				
（盖章）（盖章）				

5.5.6重保要求

在国家重大活动和重大突发事件期间，采购人接上级主管部门要求要开展值班值守和重点保障工作的，投标人需提供专业技术人员，配合采购人开展本项目基础设施、应用系统和网络安全的重保工作。工作内容包括但不限于7*24系统状态监控、安全漏洞排查与修复、应急响应、定时汇报和现场值守等。

5.5.7廉政要求

投标人与采购人签订廉政责任书（反商业贿赂协议，见合同附件）。

5.5.8归档要求

投标人需按照广东省政务服务和数据管理局及采购人的项目归档有关要求，在项目完成验收后的20个工作日内协助采购人完成项目成果资料归档工作。

5.5.9其它约定

其他未涉及内容参照本项目采购文件中技术服务合同文本相应条款的约定执行。

采购包1（广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务））

1.主要商务要求

标的提供的时间	第1种模式：以采购人确认的服务启动报审备案时间为服务起始时间，服务期为12个月。服务起始时间不晚于2026年10月1日。第2种模式：自2027年4月27日开始，至2027年10月27日止，共6个月。其中，一体化平台中云GIS模块的运行维护周期按第1种模式。具体见采购需求中的服务期限章节。
标的提供的地点	广东省广州市。
付款方式	1期：支付比例30%,本项目签订合同生效后，中标人书面提出支付申请书及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的30%。 2期：支付比例10%,2026年11月10日前，采购人对截至2026年10月31日的项目实施成果进行阶段性考核，根据考核情况对投标人的服务质量打分，并根据评价结果确定项目进度款支付金额。中标人书面提出支付申请书及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的10%。 3期：支付比例20%,2027年3月31日前，采购人对2026年11月至2027年2月的项目实施成果进行阶段性考核，根据考核情况对投标人的服务质量打分，并根据评价结果确定项目进度款支付金额。中标人书面提出支付申请书及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的20%。 4期：支付比例20%,2027年6月30日前，采购人对2027年3月至2027年5月的项目实施成果进行阶段性考核，根据考核情况对投标人的服务质量打分，并根据评价结果确定项目进度款支付金额。中标人书面提出支付申请书及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的20%。 5期：支付比例20%,项目最终验收通过后，采购人根据考核情况对中标人的服务质量打分，并根据评价结果、实际服务期确定项目尾款支付金额。中标人书面提出支付申请书及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付2027年度应付款项的20%。 如项目发生合同融资，采购人需将合同款项支付到合同约定收款账户
验收要求	1期：1.验收标准和条件 （1）符合本项目采购文件中采购需求描述相关技术要求和中标人投标文件中承诺的相应技术指标或标准。（2）采购人与中标人在项目实施过程中约定的其他相关技术要求。2.验收方式 由采购人组织专家进行验收，必要时，可邀请第三方机构进行验收。3.验收期限 项目服务期满之日起30个工作日内完成验收。验收前10个工作日，按采购人要求提交本项目验收前置审核有关成果资料。4.成果交付期限 本项目通过验收之日起10个工作日内。
履约保证金	不收取
其他	

2.技术标准与要求

序号	品目名称	标的名称	单位	数量	分项预算单价 (元)	分项预算总价 (元)	所属行业	技术要求
1	计算机设备和软件租赁服务	专业基础设施服务	项	1.00	5,964,400.00	5,964,400.00	软件和信息技术服务业	详见附件一
2	计算机设备和软件租赁服务	成品软件租赁服务（许可）服务	项	1.00	350,000.00	350,000.00	软件和信息技术服务业	详见附件二
3	其他运行维护服务	基础设施运行维护、软件系统运行维护、其他运行维护服务	项	1.00	8,664,300.00	8,664,300.00	软件和信息技术服务业	详见附件三

附表一：专业基础设施服务

参数性质	序号	具体技术(参数)要求
	1	见一、项目概况所属内容。
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。 打“▲”号条款为重要技术参数，若有部分“▲”条款未响应或不满足，不作为无效投标条款。	

附表二：成品软件租赁服务（许可）服务

参数性质	序号	具体技术(参数)要求
	1	见一、项目概况所属内容。
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。 打“▲”号条款为重要技术参数，若有部分“▲”条款未响应或不满足，不作为无效投标条款。	

附表三：基础设施运行维护、软件系统运行维护、其他运行维护服务

参数性质	序号	具体技术(参数)要求
	1	见一、项目概况所属内容。
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。 打“▲”号条款为重要技术参数，若有部分“▲”条款未响应或不满足，不作为无效投标条款。	

第三章 投标人须知

投标人必须认真阅读招标文件中所有的事项、格式、条款和采购需求等。投标人没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件在各方面都做出实质性响应的可能导致其投标无效或被拒绝。

请注意：供应商需在投标文件截止时间前，将加密投标文件上传至云平台项目采购系统中并取得回执，逾期上传或错误方式投递送达将导致投标无效。

一、名词解释

1.采购代理机构：本项目是指广东志正招标有限公司，负责整个采购活动的组织，依法负责编制和发布招标文件，对招标文件拥有最终的解释权，不以任何身份出任评标委员会成员。

2.采购人：本项目是指广东省国土资源技术中心（广东省基础地理信息中心），是采购活动当事人之一，负责项目的整体规划、技术方案可行性设计论证与实施，作为合同采购方（用户）的主体承担质疑回复、履行合同、验收与评价等义务。

3.投标人：是指在云平台项目采购系统完成本项目投标登记并提交电子投标文件的供应商。

4.“评标委员会”是指根据《中华人民共和国政府采购法》等法律法规规定，由采购人代表和有关专家组成以确定中标供应商或者推荐中标候选人的临时组织。

5.“中标供应商”是指经评标委员会评审确定的对招标文件做出实质性响应，经采购人按照规定在评标委员会推荐的中标候选人中确定的或评标委员会受采购人委托直接确认的投标人。

6.招标文件：是指包括招标公告和招标文件及其补充、变更和澄清等一系列文件。

7.电子投标文件：是指使用云平台提供的投标客户端制作加密并上传到系统的投标文件。（投标客户端制作投标文件时，生成的后缀为“.标书”的文件）

8.备用电子投标文件：是指使用云平台提供的投标客户端制作电子投标文件时，同时生成的同一版本的备用投标文件。（投标客户端制作投标文件时，生成的后缀为“.备用标书”的文件）

9.电子签名和电子印章：是指获得中华人民共和国工业和信息化部颁发的《电子认证服务许可证》、国家密码管理局颁发的《电子认证服务使用密码许可证》的资质，具备承担因数字证书原因产生纠纷的相关责任的能力，且在广东省内具有数量基础和服务能力的依法设立电子认证服务机构签发的电子签名和电子签章认证证书（即CA数字证书）。供应商应当到相关服务机构办理并取得数字证书介质和应用。电子签名包括单位法定代表人、被委托人及其他个人的电子形式签名；电子印章包括机构法人电子形式印章。电子签名及电子印章与手写签名或者盖章具有同等的法律效力。签名（含电子签名）和盖章（含电子印章）是不同使用场景，应按招标文件要求在投标（响应）文件指定位置进行签名（含电子签名）和盖章（含电子印章），对允许采用手写签名的文件，应在纸质文件手写签名后，提供文件的彩色扫描电子文档进行后续操作。

10.“全称”、“公司全称”、“加盖单位公章”及“公章”：在电子投标（响应）文件及相关的其他电子资料中，涉及“全称”或“公司全称”的应在对应文件编辑时使用文本录入方式，或在纸质投标（响应）文件上进行手写签名，或通过投标客户端使用电子印章完成；涉及“加盖单位公章”和“公章”应使用投标人单位的数字证书并通过投标客户端使用电子印章完成。

11.“投标人代表签字”及“授权代表”：在电子投标（响应）文件及相关的其他电子资料中，涉及“投标人代表签字”或“授权代表”应在投标（响应）文件编辑时使用文本录入方式，或在纸质投标（响应）文件上进行手写签名，或通过投标客户端使用电子签名完成。

12.“法定代表人”：在电子投标（响应）文件及相关的其他电子资料中，涉及“法定代表人”应在纸质投标（响应）文件上进行手写签名，或通过投标客户端使用电子签名完成。

13.日期、天数、时间：未有特别说明时，均为公历日（天）及北京时间。

二、须知前附表

本表与招标文件对应章节的内容若不一致，以本表为准。

序号	条款名称	内容及要求
1	采购包情况	本项目共1个采购包
2	开标方式	远程电子开标
3	评标方式	现场电子评标（供应商应当审慎标记各评审项的应答部分，标记内容清晰且完整，否则将自行承担不利后果）
4	评标办法	采购包1：综合评分法
5	报价形式	采购包1：总价
6	报价要求	各采购包报价不超过预算总价
7	现场踏勘	否
8	投标有效期	从提交投标（响应）文件的截止之日起90日历天
9	投标保证金	采购包1：保证金人民币140000.0元整 缴费渠道：电子保函（保险）、支票（本票、汇票）、其他 开户单位：广东志正招标有限公司 开户账号：800201177509011 开户银行：广州银行股份有限公司龙口西支行 支票提交方式：保证金相关事宜联系人：廖小姐 联系电话：020-87554268 汇票、本票提交方式：保证金相关事宜联系人：廖小姐 联系电话：020-87554268 投标保证金有效期：与投标有效期一致。 投标保函提交方式：供应商可通过"广东政府采购智慧云平台金融服务中心"(http://gdgpo.czt.gd.gov.cn/zcdservice/zcd/guangdong/)，申请办理投标（响应）担保函、保险（保证）凭证，成功出函的等效于现金缴纳投标保证金。 投标保证金有效期:与投标有效期一致。 投标保函提交方式：供应商可通过"广东政府采购智慧云平台金融服务中心"(https://gdgpo.czt.gd.gov.cn/zcdservice/zcd/guangdong/)，申请办理投标（响应）担保函、保险（保证）凭证，成功出函的等效于现金缴纳投标保证金。
10	投标文件要求	一、电子投标文件（必须提供）： （1）加密的电子投标文件 1 份（需在递交投标文件截止时间前成功上传至云平台项目采购系统）。 （2）非加密电子版文件 U 盘(或光盘) 0 份，加密的电子投标文件与非加密的电子投标文件必须完全一致。 非加密电子版投标文件使用情形：当无法使用 CA 证书在云平台项目采购系统进行电子投标文件开标解密时，供应商须在代理机构指引下启用非加密电子版投标文件。 二、纸质投标文件（代理机构自行选择）：（3）纸质投标文件正本0份，纸质投标文件副本0份。纸质投标文件应与电子投标文件一致（递交的纸质文件需密封完好，注明“正本”和“副本”字样，正本和副本分别封装。如果正本与副本不符，应以正本为准。）。纸质投标文件使用情形：当项目采购系统出现故障，无法使用电子投标文件评标时，代理机构可根据云平台发布的通知指引，根据实际情况使用纸质投标文件评标。 在电子投标文件能正常使用的情况下，不得因供应商未提交纸质投标文件而认定供应商投标无效。
11	中标候选人推荐家数	采购包1： 2家

12	中标供应商数量	采购包1： 1家
13	有效供应商家数	采购包1： 3家 此人数约定了开标与评标过程中的最低有效供应商家数，当家数不足时项目将不得开标、不得评标或直接废标。
14	项目兼投兼中（兼投不兼中）规则	无： -
15	中标供应商确定方式	采购人按照评审报告中推荐的成交候选人确定中标（成交）人。
16	代理服务费	收取。 采购机构代理服务收费标准：中标人须向采购代理机构按如下标准和规定缴纳招标代理服务费： （1）以中标总金额作为招标代理服务费的计算基数；（2）招标代理服务费采用差额定率累进法进行计算，按照以下标准计取：100万元以下的部分，按照1.5%计取；100-500万元的部分，按照0.8%计取；500-1000万元的部分，按照0.45%计取；1000-5000万元的部分，按照0.25%计取。（3）增值税另行计入招标代理服务费中。
17	代理服务费收取方式	向中标/成交供应商收取
18	其他	
19	开标解密时长	说明：具体情况根据开标时现场代理机构人员设置为准 说明：具体情况根据开标时现场代理机构人员设置为准
20	专门面向中小企业采购	采购包1：面向中小企业，以合同分包形式预留，预留比例：40%。

三、说明

1.总则

采购人、采购代理机构及投标人进行的本次采购活动适用《中华人民共和国政府采购法》及其配套的法规、规章、政策。

投标人应仔细阅读本项目招标公告及招标文件的所有内容（包括变更、补充、澄清以及修改等，且均为招标文件的组成部分），按照招标文件要求以及格式编制投标文件，并保证其真实性，否则一切后果自负。

本次公开招标项目，是以招标公告的方式邀请非特定的投标人参加投标。

2.适用范围

本招标文件仅适用于本次招标公告中所涉及的项目和内容。

3.进口产品

若本项目允许采购进口产品，供应商应保证所投产品可履行合法报通关手续进入中国关境内。

若本项目不允许采购进口产品，如供应商所投产品为进口产品，其响应将被认定为响应无效。

4.投标的费用

不论投标结果如何，投标人应承担所有与准备和参加投标有关的费用。采购代理机构和采购人均无义务和责任承担相关费用。

5.以联合体形式投标的，应符合以下规定：

5.1联合体各方均应当满足《中华人民共和国政府采购法》第二十二条规定的条件，并在投标文件中提供联合体各方的相关

证明材料。

5.2 联合体各方之间应签订共同投标协议书并在投标文件中提交，明确约定联合体各方承担的工作和相应的责任。联合体各方签订共同投标协议书后，不得再以自己名义单独在同一项目（采购包）中投标，也不得组成新的联合体参加同一项目（采购包）投标，若违反规定则其参与的所有投标将视为无效投标。

5.3 联合体应以联合协议中确定的牵头方名义登录云平台项目采购系统进行项目投标，录入联合体所有成员单位的全称并使用成员单位的电子印章进行联投确认，联合体名称需与共同投标协议书签署方一致。对于需交投标保证金的，以牵头方名义缴纳。

5.4 联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

5.5 联合体各方均应满足《中华人民共和国政府采购法》第二十二条规定的条件。根据《中华人民共和国政府采购法实施条例》第二十二条，联合体中有同类资质的供应商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供应商确定资质等级。

5.6 联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任。

6.关联企业投标说明

6.1 对于不接受联合体投标的采购项目（采购包）：法定代表人或单位负责人为同一个人或者存在直接控股、管理关系的不同供应商，不得同时参加同一项目或同一采购包的投标。如同时参加，则其投标将被拒绝。

6.2 对于接受联合体投标的采购项目（采购包）：除联合体外，法定代表人或单位负责人为同一个人或者存在直接控股、管理关系的不同供应商，不得同时参加同一项目或同一采购包的投标。如同时参加，则评审时将同时被拒绝。

7.关于中小微企业投标

中小微企业响应是指在政府采购活动中，供应商提供的货物均由中小微企业制造、工程均由中小微企业承建或者服务均由中小微企业承接，并在响应文件中提供《中小企业声明函》。本条款所称中小微企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。中小企业划分见《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）。

根据财库〔2014〕68号《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》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业投标时，提供由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，不再提供《中小企业声明函》。

根据财库〔2017〕141号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受政府采购支持政策的残疾人福利性单位应当同时满足《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》所列条件。残疾人福利性单位属于小型、微型企业的，不重复享受政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》，并对声明的真实性负责。

8.纪律与保密事项

8.1 投标人不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人或其他投标人的合法权益，投标人不得以向采购人、评标委员会成员行贿或者采取其他不正当手段谋取中标。

8.2 在确定中标供应商之前，投标人不得与采购人就投标价格、投标方案等实质性内容进行谈判，也不得私下接触评标委员会成员。

8.3 在确定中标供应商之前，投标人试图在投标文件审查、澄清、比较和评价时对评标委员会、采购人和采购代理机构施加任何影响都可能导致其投标无效。

8.4 获得本招标文件者，须履行本项目下保密义务，不得将因本次项目获得的信息向第三人外传，不得将招标文件用作本次投标以外的任何用途。

8.5由采购人向投标人提供的图纸、详细资料、样品、模型、模件和所有其它资料，均为保密资料，仅被用于它所规定的用途。除非得到采购人的同意，不能向任何第三方透露。开标结束后，应采购人要求，投标人应归还所有从采购人处获得的保密资料。

8.6采购人或采购代理机构有权将供应商提供的所有资料向有关政府部门或评审小组披露。

8.7在采购人或采购代理机构认为适当时、国家机关调查、审查、审计时以及其他符合法律规定的情形下，采购人或采购代理机构无须事先征求供应商同意而可以披露关于采购过程、合同文本、签署情况的资料、供应商的名称及地址、响应文件的有关信息以及补充条款等，但应当在合理的必要范围内。对任何已经公布过的内容或与之内容相同的资料，以及供应商已经泄露或公开的，无须再承担保密责任。

9.语言文字以及度量衡单位

9.1除招标文件另有规定外，投标文件应使用中文文本，若有不同文本，以中文文本为准。投标文件提供的全部资料中，若原件属于非中文描述，应提供具有翻译资质的机构翻译的中文译本。前述翻译机构应为中国翻译协会会员单位，翻译的中文译本应由翻译人员签名并加盖翻译机构公章，同时提供翻译人员翻译资格证书。中文译本、翻译机构的成员单位证书及翻译人员的资格证书可为复印件。

9.2除非招标文件的技术规格中另有规定，投标人在投标文件中及其与采购人和采购代理机构的所有往来文件中的计量单位均采用中华人民共和国法定计量单位。

9.3投标人所提供的货物和服务均应以人民币报价，货币单位：元。

10. 现场踏勘（如有）

10.1招标文件规定组织踏勘现场的，采购人按招标文件规定的时间、地点组织投标人踏勘项目现场。

10.2投标人自行承担踏勘现场发生的责任、风险和自身费用。

10.3采购人在踏勘现场中介绍的资料和数据等，只是为了使投标人能够利用招标人现有的资料。招标人对投标人由此而作出的推论、解释和结论概不负责。

四、招标文件的澄清和修改

1.采购代理机构对招标文件进行必要的澄清或者修改的，在指定媒体上发布更正公告。澄清或者修改的内容可能影响投标文件编制的，更正公告在投标截止时间至少15日前发出；不足15日的，代理机构顺延提交投标文件截止时间。

2.更正公告及其所发布的内容或信息（包括但不限于：招标文件的澄清或修改、现场考察或答疑会的有关事宜等）作为招标文件的组成部分，对投标人具有约束力。一经在指定媒体上发布后，更正公告将作为通知所有招标文件收受人的书面形式。

3.如更正公告有重新发布电子招标文件的，供应商应登录云平台项目采购系统下载最新发布的电子招标文件制作投标文件。

4.投标人在规定的时间内未对招标文件提出疑问、质疑或要求澄清的，将视其为无异议。对招标文件中描述有歧义或前后不一致的地方，评标委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

五、投标要求

1.投标登记

投标人应从广东省政府采购网（<https://gdgpo.czt.gd.gov.cn/>）上广东政府采购智慧云平台（以下简称“云平台”）的政府采购供应商入口进行免费注册后，登录进入项目采购系统完成项目投标登记并在线获取招标文件（未按上述方式获取招标文件的供应商，其投标资格将被视为无效）。

2.投标文件的制作

2.1投标文件中，所有内容均以电子文件编制，其格式要求详见第六章说明。如因不按要求编制导致系统无法检索、读取相关信息时，其后果由投标人承担。由于本项目采用电子化投标，请充分考虑设备、网络环境、人员对系统熟悉度等因素，合理安排投标文件制作、提交时间，建议至少提前一天完成制作、提交工作。

2.2 投标人应使用云平台提供的投标客户端编制、标记、加密投标文件，成功加密后将生成指定格式的电子投标文件和电子备用投标文件。所有投标文件不能进行压缩处理。关于电子投标报价（如有报价）说明如下：

(1) 投标人应按照“第二章采购需求”的需求内容、责任范围以及合同条款进行报价。并按“开标一览表”和“分项报价表”规定的格式报出总价和分项价格。投标总价中不得包含招标文件要求以外的内容，否则，在评审时不予核减。

(2) 投标报价包括本项目采购需求和投入使用的所有费用，包括但不限于主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

2.3 如有对多个采购包投标的，要对每个采购包独立制作电子投标文件。

2.4 投标人不得将同一个项目或同一个采购包的内容拆开投标，否则其报价将被视为非实质性响应。

2.5 投标人须对招标文件的对应要求给予唯一的实质性响应，否则将视为不响应。

2.6 招标文件中，凡标有“★”的地方均为实质性响应条款，投标人若有一项带“★”的条款未响应或不满足，将按无效投标处理。

2.7 投标人必须按招标文件指定的格式填写各种报价，各报价应计算正确。除在招标文件另有规定外（如：报折扣、报优惠率等），计量单位应使用中华人民共和国法定计量单位，以人民币填报所有报价。

2.8 投标文件以及投标人与采购人、代理机构就有关投标的往来函电均应使用中文。投标人提交的支持性文件和印制的文件可以用另一种语言，但相应内容应翻译成中文，在解释投标文件时以中文文本为准。

2.9 投标人应按招标文件的规定及附件要求的内容和格式完整地填写和提供资料。投标人必须对投标文件所提供的全部资料的真实性承担法律责任，并无条件接受采购人和政府采购监督管理部门对其中任何资料进行核实（核对原件）的要求。采购人核对发现有不一致或供应商无正当理由不按时提供原件的，应当书面知会代理机构，并书面报告本级人民政府财政部门。

3. 投标文件的提交

3.1 在投标文件提交截止时间前，投标人须将电子投标文件成功完整上传到云平台项目采购系统，且取得投标回执。时间以云平台项目采购系统服务器从中国科学院国家授时中心取得的北京时间为准，投标截止时间结束后，系统将不允许投标人上传投标文件，已上传投标文件但未完成传输的文件系统将拒绝接收。

3.2 代理机构对因不可抗力事件造成的投标文件的损坏、丢失的，不承担责任。

3.3 出现下述情形之一，属于未成功提交投标文件，按无效投标处理：

（1）至提交投标文件截止时，投标文件未完整上传的。

（2）投标文件未按投标格式中注明需签字盖章的要求进行签名（含电子签名）和加盖电子印章，或签名（含电子签名）或电子印章不完整的。

（3）投标文件损坏或格式不正确的。

4. 投标文件的修改、撤回与撤销

4.1 在提交投标文件截止时间前，投标人可以修改或撤回未解密电子投标文件，并于提交投标文件截止时间前将修改后重新生成的电子投标文件上传至系统，到达投标文件提交截止时间后，将不允许修改或撤回。

4.2 在提交投标文件截止时间后，投标人不得补充、修改和更换投标文件。

5. 投标文件的解密

到达开标时间后，投标人需携带并使用制作该投标文件的同一数字证书参加开标解密，投标人须在采购代理机构规定的时间内完成投标文件解密，投标人未携带数字证书或其他非系统原因导致的逾期未解密投标文件，将作无效投标处理。

6. 投标保证金

6.1 投标保证金的缴纳

投标人在提交投标文件时，应按投标人须知前附表规定的金额和缴纳要求缴纳投标保证金，并作为其投标文件的组成部分。

如采用转账、支票、本票、汇票形式提交的，投标保证金从投标人基本账户递交，由广东志正招标有限公司代收。具体操

作要求详见广东志正招标有限公司有关指引，递交事宜请自行咨询广东志正招标有限公司；请各投标人在投标文件递交截止时间前按须知前附表规定的金额递交至广东志正招标有限公司，到账情况以开标时广东志正招标有限公司查询的信息为准。

如采用金融机构、专业担保机构开具的投标担保函、投标保证保险函等形式提交投标保证金的，投标担保函或投标保证保险函须开具给采购人（保险受益人须为采购人），并与投标文件一同递交。

投标人可通过"广东政府采购智慧云平台金融服务中心"(<https://gdgpo.czt.gd.gov.cn/zcdservice/zcd/guangdong/>)，申请办理电子保函，电子保函与纸质保函具有同样效力。

注意事项：供应商通过线下方式缴纳保证金（转账、支票、汇票、本票、纸质保函）的，需准备缴纳凭证的扫描件作为核验凭证；通过电子保函形式缴纳保证金的，如遇开标或评标现场无法拉取电子保函信息时，可提供电子保函打印件或购买凭证作为核验凭证。相关凭证应上传至系统归档保存。

6.2投标保证金的退还：

- （1）投标人在投标截止时间前放弃投标的，自所投采购包结果公告发出后5个工作日内退还。
- （2）未中标的投标人投标保证金，自中标通知书发出之日起5个工作日内退还。
- （3）中标供应商的投标保证金，自政府采购合同签订之日起5个工作日内退还。

备注：但因投标人自身原因导致无法及时退还的除外。

6.3有下列情形之一的，投标保证金将不予退还：

- （1）提供虚假材料谋取中标、成交的；
- （2）投标人在招标文件规定的投标有效期内撤销其投标；
- （3）中标后，无正当理由放弃中标资格；
- （4）中标后，无正当理由不与采购人签订合同；
- （5）法律法规和招标文件规定的其他情形。

7.投标有效期

7.1投标有效期内投标人撤销投标文件的，采购人或者采购代理机构可以不退还投标保证金（如有）。采用投标保函方式替代保证金的，采购人或者采购代理机构可以向担保机构索赔保证金。

7.2出现特殊情况需延长投标有效期的，采购人或采购代理机构可于投标有效期满之前要求投标人同意延长有效期，要求与答复均以书面形式通知所有投标人。投标人同意延长的，应相应延长其投标保证金（如有）的有效期，但不得要求或被允许修改或撤销其投标文件；投标人可以拒绝延长有效期，但其投标将会被视为无效，拒绝延长有效期的投标人有权收回其投标保证金（如有）。采用投标保函方式替代保证金的，投标有效期超出保函有效期的，采购人或者采购代理机构应提示投标人重新开函，未获得有效保函的投标人其投标将会被视为无效。

8.样品（演示）

8.1招标文件规定投标人提交样品的，样品属于投标文件的组成部分。样品的生产、运输、安装、保全等一切费用由投标人自理。

8.2投标截止时间前，投标人应将样品送达至指定地点。若需要现场演示的，投标人应提前做好演示准备（包括演示设备）。

8.3采购结果公告发布后，中标供应商的样品由采购人封存，作为履约验收的依据之一。未中标供应商在接到采购代理机构通知后，应按规定时间尽快自行取回样品，否则视同供应商不再认领，代理机构有权进行处理。

9.除招标文件另有规定外，有下列情形之一的，投标无效：

- 9.1投标文件未按照招标文件要求签署、盖章；
- 9.2不符合招标文件中规定的资格要求；
- 9.3投标报价超过招标文件中规定的预算金额或最高限价；
- 9.4投标文件含有采购人不能接受的附加条件；
- 9.5有关法律、法规和规章及招标文件规定的其他无效情形。

六、开标、评标和定标

1. 开标

1.1 开标程序

招标工作人员按招标公告规定的时间进行开标，由采购人或者采购代理机构工作人员宣布投标人名称、解密情况，投标价格和招标文件规定的需要宣布的其他内容（以开标一览表要求为准）。开标分为现场电子开标和远程电子开标两种。

采用现场电子开标的：投标人的法定代表人或其委托代理人应当按照本招标公告载明的时间和地点前往参加开标，并携带编制本项目（采购包）电子投标文件时加密所用的数字证书、存储有备用电子投标文件的U盘前往开标现场。

采用远程电子开标的：投标人的法定代表人或其授权代表应当按照本招标公告载明的时间和模式等要求参加开标。在投标截止时间前30分钟，应当登录云平台开标大厅进行签到，并且填写授权代表的姓名与手机号码。若因签到时填写的授权代表信息有误而导致的不良后果，由供应商自行承担。

开标时，投标人应当使用编制本项目（采购包）电子投标文件时加密所用数字证书在开始解密后按照代理机构规定的时间内完成电子投标文件的解密，如遇不可抗力等其他特殊情况，采购代理机构可视情况延长解密时间。投标人未携带数字证书或其他非系统原因导致的在规定时间内未解密投标文件，将作无效投标处理。（采用远程电子开标的，各投标人在参加开标以前须自行对使用电脑的网络环境、驱动安装、客户端安装以及数字证书的有效性等进行检测，确保可以正常使用）。

如在电子开标过程中出现无法正常解密的，代理机构可根据实际情况开启上传备用电子投标文件通道。系统将对上传的备用电子投标文件的合法性进行验证，若发现提交的备用电子投标文件与加密的电子投标文件版本不一致（即两份文件不是通过投标客户端同时加密生成的），系统将拒绝接收，视为无效投标。如供应商无法在代理规定的时间内完成备用电子投标文件的上传，投标将被拒绝，作无效投标处理。

1.2 开标异议

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的，应当场提出询问或者回避申请。投标人未参加开标的，视同认可开标结果。

1.3 投标截止时间后，投标人不足须知前附表中约定的有效供应商家数的，不得开标。同时，本次采购活动结束。

1.4 开标时出现下列情况的，视为投标无效处理：

（1）经检查数字证书无效的；

（2）因投标人自身原因，未在规定时间内完成电子投标文件解密的；

（3）如需使用备用电子投标文件解密时，在规定的解密时间内无法提供备用电子投标文件或提供的备用电子投标文件与加密的电子投标文件版本不一致（即两份文件不是通过投标客户端同时加密生成的）。

2. 评审（详见第四章）

3. 定标

3.1 中标公告：

中标供应商确定之日起2个工作日内，采购人或采购代理机构将在中国政府采购网(www.ccgp.gov.cn)、广东省政府采购网(<https://gdgpo.czt.gd.gov.cn/>)广东志正招标有限公司（<https://www.zztender.com/>）上以公告的形式发布中标结果，中标公告的公告期限为1个工作日。中标公告同时作为采购代理机构通知除中标供应商外的其他投标人没有中标的书面形式，采购代理机构不再以其它方式另行通知。

3.2 中标通知书：

中标通知书在发布中标公告时，在云平台同步发送至中标供应商。中标供应商可在云平台自行下载打印《中标通知书》，《中标通知书》将作为授予合同资格的唯一合法依据。中标通知书发出后，采购人不得违法改变中标结果，中标供应商不得放弃中标。中标供应商放弃中标的，应当依法承担相应的法律责任。

3.3 终止公告：

项目废标后，采购人或采购代理机构将在中国政府采购网(www.ccgp.gov.cn)、广东省政府采购网

(<https://gdgpo.czt.gd.gov.cn/>)、广东志正招标有限公司 (<https://www.zztender.com/>) 上发布终止公告，终止公告的公告期限为1个工作日。

七、询问、质疑与投诉

1. 询问

投标人对政府采购活动事项（招标文件、采购过程和中标结果）有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构将及时作出答复，但答复的内容不涉及商业秘密。询问可以口头方式提出，也可以书面方式提出，书面方式包括但不限于传真、信函、电子邮件。联系方式见《投标邀请函》中“采购人、采购代理机构的名称、地址和联系方式”。

2. 质疑

2.1 供应商认为招标文件、采购过程和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七个工作日内，以书面原件形式向采购人或采购代理机构一次性提出针对同一采购程序环节的质疑，逾期质疑无效。供应商应知其权益受到损害之日是指：

(1) 对招标文件提出质疑的，为获取招标文件之日或者招标文件公告期限届满之日；

(2) 对采购过程提出质疑的，为各采购程序环节结束之日；

(3) 对中标结果提出质疑的，为中标结果公告期限届满之日。

2.2 质疑函应当包括下列主要内容：

(1) 质疑供应商和相关供应商的名称、地址、邮编、联系人及联系电话等；

(2) 质疑项目名称及编号、具体明确的质疑事项和与质疑事项相关的请求；

(3) 认为采购文件、采购过程、中标和成交结果使自己的合法权益受到损害的法律依据、事实依据、相关证明材料及证据来源；

(4) 提出质疑的日期。

2.3 质疑函应当署名。质疑供应商为自然人的，应当由本人签字；质疑供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

2.4 以联合体形式参加政府采购活动的，其质疑应当由联合体成员委托主体提出。

2.5 供应商质疑应当有明确的请求和必要的证明材料。质疑内容不得含有虚假、恶意成份。依照谁主张谁举证的原则，提出质疑者必须同时提交相关确凿的证据材料和注明证据的确切来源，证据来源必须合法，采购人或采购代理机构有权将质疑函转发质疑事项各关联方，请其作出解释说明。对捏造事实、滥用维权扰乱采购秩序的恶意质疑者，将上报政府采购监督管理部门依法处理。

2.6 质疑联系方式如下：

质疑联系人：内控部

电话：020-87512543

传真：87554028

邮箱：nkb@zztender.com

地址：广东省广州市天河区龙怡路117号银汇大厦5楼

邮编：510640

3. 投诉

质疑人对采购人或采购代理机构的质疑答复不满意或在规定时间内未得到答复的，可以在答复期满后15个工作日内，按如下联系方式向本项目监督管理部门提起投诉。

政府采购监督管理机构名称：广东省财政厅政府采购监管处

地 址：广州市越秀区北京路376号北裙楼313室

电 话：020-83340570

八、合同签订和履行

1.合同签订

1.1采购人应当自《中标通知书》发出之日起三十日内，按照招标文件和中标供应商投标文件的约定，与中标供应商签订合同。所签订的合同不得对招标文件和中标供应商投标文件作实质性修改。超过30天尚未完成政府采购合同签订的政府采购项目，采购人应当登录广东省政府采购网，填报未能依法签订政府采购合同的具体原因、整改措施和预计签订合同时间等信息。

1.2采购人不得提出试用合格等任何不合理的要求作为签订合同的条件，且不得与中标供应商私下订立背离合同实质性内容的协议。

1.3合同条款中应规定，乙方完全遵守《中华人民共和国民法典》有关规定和《中华人民共和国妇女权益保障法》中关于“劳动和社会保障权益”的有关要求。

1.4采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

1.5采购人应当自政府采购合同签订之日起2个工作日内，登录广东省政府采购网上传政府采购合同扫描版，如实填报政府采购合同的签订时间。依法签订的补充合同，也应在补充合同签订之日起2个工作日内公开并备案采购合同。

2.合同的履行

2.1政府采购合同订立后，合同各方不得擅自变更、中止或者终止合同。

2.2政府采购合同履行中，采购人需追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与成交供应商签订补充合同，但所补充合同的采购金额不得超过原采购金额的10%。依法签订的补充合同，也应在补充合同签订之日起2个工作日内登录广东省政府采购网上传备案。

第四章 评标

一、评标要求

1.评标方法

采购包1(广东省国土资源技术中心政务信息化运维(2026年)项目(基础设施及运行维护服务)): 综合评分法,是指投标文件满足招标文件全部实质性要求,且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。(最低报价不是中标的唯一依据。)

2.评标原则

2.1评标活动遵循公平、公正、科学和择优的原则,以招标文件和投标文件为评标的基本依据,并按照招标文件规定的评标方法和评标标准进行评标。

2.2具体评标事项由评标委员会负责,并按招标文件的规定办法进行评审。

2.3合格投标人不足须知前附表中约定的有效供应商家数的,不得评标。

3.评标委员会

3.1评标委员会由采购人代表和评审专家组成,成员人数应当为5人及以上单数,其中评审专家不得少于成员总数的三分之二。

3.2评标应遵守下列评标纪律:

(1) 评标情况不得私自外泄,有关信息由广东志正招标有限公司统一对外发布。

(2) 对广东志正招标有限公司或投标人提供的要求保密的资料,不得摘记翻印和外传。

(3) 不得收受投标供应商或有关人员的任何礼物,不得串联鼓动其他人袒护某投标人。若与投标人存在利害关系,则应主动声明并回避。

(4) 全体评委应按照招标文件规定进行评标,一切认定事项应查有实据且不得弄虚作假。

(5) 评标委员会各成员应当独立对每个投标人的投标文件进行评价,并对评价意见承担个人责任。评审过程中,不得发表倾向性言论。

※对违反评标纪律的评委,将取消其评委资格,对评标工作造成严重损失者将予以通报批评乃至追究法律责任。

4.有下列情形之一的,视为投标人串通投标,其投标无效:

4.1不同投标人的投标文件由同一单位或者个人编制;

4.2不同投标人委托同一单位或者个人办理投标事宜;

4.3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;

4.4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;

4.5不同投标人的投标文件相互混装;

4.6不同投标人的投标保证金或购买电子保函支付款为从同一单位或个人的账户转出;

4.7投标人上传的电子投标文件加盖该项目的其他投标人的电子印章的。

说明:在评标过程中发现投标人有上述情形的,评标委员会应当认定其投标无效。同时,项目评审时被认定为串通投标的投标人不得参加该合同项下的采购活动。

5.投标无效的情形

详见资格性审查、符合性审查和招标文件其他投标无效条款。

6.定标

评标委员会按照招标文件确定的评标方法、步骤、标准,对投标文件进行评审。评标结束后,对投标人的评审名次进行排序,确定中标供应商或者推荐中标候选人。

7.价格修正

对报价的计算错误按以下原则修正：

- （1）投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准；
- （2）大写金额和小写金额不一致的，以大写金额为准；
- （3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。
- （4）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。但是单价金额计算结果超过预算价的，对其按无效投标处理。

- （5）若投标客户端上传的电子报价数据与电子投标文件价格不一致的，以电子报价数据为准。

注：同时出现两种以上不一致的，按照前款规定的顺序在系统上进行价格澄清。澄清后的价格加盖电子印章确认后产生约束力，但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，投标人不确认的，其投标无效。

二.政府采购政策落实

1.节能、环保要求

采购的产品属于品目清单范围的，将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购，具体按照本招标文件相关要求执行。

相关认证机构和获证产品信息以市场监管总局组织建立的节能产品、环境标志产品认证结果信息发布平台公布为准。

2.对符合本国产品标准的产品给予价格扣除

依照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）及《财政部关于贯彻落实<国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知>的意见》（财库〔2025〕30号）等相关规定。

（1）**本国产品标准的适用范围。**本国产品标准适用于货物，包括政府采购货物项目和服务项目中涉及的货物。适用本国产品标准的货物具体是指《政府采购品目分类目录》中的货物类产品，但不包括其中的房屋和构筑物，文物和陈列品，图书和档案，特种动植物，农林牧渔业产品，矿与矿物，电力、城市燃气、蒸汽和热水、水，食品、饮料和烟草原料，无形资产。

（2）**准确界定产品在中国境内生产。**本国产品应当在中国境内生产，即在中华人民共和国关境内实现从原材料、组件到产品的属性改变。从具体情形看，在国内保税区、综合保税区等海关特殊监管区域生产的产品，属于在中国境内生产的产品；对医疗器械产品，取得药品监督管理部门授予的准字号医疗器械注册证的，属于在中国境内生产的产品；其他产品，根据实际情况判断是否在中国境内生产。

（3）**对本国产品的支持政策。**政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠，对本国产品的报价给予20%的价格扣除，用扣除后的价格参与评审。

当采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到80%以上时，依法对该供应商提供的全部产品给予价格评审优惠，即对该供应商提供的全部产品的总报价给予20%的价格扣除，用扣除后的价格参与评审。

（4）**认真审查有关证明文件。**采购人应当在采购文件中明确对供应商所出具的《关于符合本国产品标准的声明函》（以下简称《声明函》）的完整性、准确性进行审查的要求，评审中发现《声明函》内容含义不明确、同类事项与投标（响应）文件表述不一致或者有明显文字错误等情况的，应当以书面形式要求供应商作出必要的澄清、说明或者补正。经澄清、说明或者补正的《声明函》仍然不符合《通知》规定要求的，供应商提供的相关产品视为不符合本国产品标准。

3.对小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除

依照《政府采购促进中小企业发展管理办法》、《支持监狱企业发展有关问题的通知》和《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》的规定，凡符合享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策的单位，按照以下比例给予相应的价格扣除：（监狱企业、残疾人福利性单位视同为小、微企业）。

4.价格扣除相关要求

采购包1（广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务））：

序号	情形	适用对象	价格扣除比例	计算公式
注：（1）上述评标价仅用于计算价格分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织、与小型、微型企业之间不得存在投资关系。				

（1）所称小型和微型企业应当符合以下条件：

在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

提供本企业（属于小微企业）制造的货物或者提供其他小型或微型企业制造的货物/提供本企业（属于小微企业）承接的服务。

（2）符合中小企业扶持政策的投标人应填写《中小企业声明函》；监狱企业须投标人提供由监狱管理局、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；残疾人福利性单位应填写《残疾人福利性单位声明函》，否则不认定价格扣除。

说明：投标人应当对其出具的《中小企业声明函》真实性负责，投标人出具的《中小企业声明函》内容不实的，属于提供虚假材料谋取中标。

（3）投标（响应）供应商统一在一份《中小企业声明函》中说明联合体各方的中小微情况：包括联合体各方均为小型、微型企业的，及中小微企业作为联合体一方参与政府采购活动，且共同投标协议书中约定，小型、微型企业的协议合同金额占到联合体协议合同总金额30%以上的。

三、评审程序

1.资格性审查、符合性审查和异常低价审查

资格性审查。公开招标采购项目开标结束后，采购人或采购代理机构应当依法对投标人的资格进行审查，以确定投标人是否具备投标资格。（详见后附表一资格性审查表）

符合性审查。评标委员会依据招标文件的规定，从投标文件的有效性、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。（详见后附表二符合性审查表）

资格性审查和符合性审查中凡有其中任意一项未通过的，评审结果为未通过，未通过资格性审查、符合性审查的投标人按无效投标处理。

异常低价审查。政府采购评审中出现采购文件明确的异常低价情形，评审委员会应当启动异常低价投标（响应）审查程序。

评审委员会启动异常低价投标（响应）审查后，应当要求相关供应商在评审现场合理的时间内对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等。

被启动异常低价审查的供应商，如果不提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，应当将其作为无效投标（响应）处理。

通过异常低价审查的不足3家，不得进入详细评审。

资格性审查、符合性审查、异常低价审查中凡有其中任意一项未通过的，评审结果为未通过，未通过资格性审查、符合性审查、异常低价审查的投标人按无效投标处理。

对各投标人进行资格审查、符合性审查、异常低价审查过程中，对初步被认定为无效投标者，由评标委员会组长或采购人代表将集体意见及时告知投标当事人。

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，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

合格投标人不足3家的，不得评标。

表一资格性审查表：

采购包1（广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务））：

序号	资格审查内容	
1	具有独立承担民事责任的能力	在中华人民共和国境内注册的法人或其他组织或自然人，投标（响应）时提交有效的营业执照（或事业法人登记证或身份证等相关证明） 副本复印件。分支机构投标的，须提供总公司和分公司营业执照副本复印件，总公司出具给分支机构的授权书。
2	有依法缴纳税收和社会保障资金的良好记录	提供投标截止日前6个月内任意1个月依法缴纳税收和社会保障资金的相关材料。如依法免税或不需要缴纳社会保障资金的，提供相应证明材料。
3	具有良好的商业信誉和健全的财务会计制度	提供2024年或2025年年度财务状况报告或投标截止日前6个月内任意1个月的财务报表复印件；或银行出具的资信证明材料复印件。
4	履行合同所必需的设备和专业技术能力	提供履行合同所必需的设备和专业技术能力情况，格式自拟。
5	参加采购活动前3年内，在经营活动中没有重大违法记录	参照投标函相关承诺格式内容。 重大违法记录，是指供应商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。（根据财库〔2022〕3号文，“较大数额罚款”认定为200万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于200万元的，从其规定）
6	信用记录	供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以资格审查人员于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网（http://www.ccgp.gov.cn/）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料）。
7	供应商必须符合法律、行政法规规定的其他条件	单位负责人为同一人或者存在直接控股、 管理关系的不同供应商，不得同时参加本采购项目（或采购包） 投标（响应）。 为本项目提供整体设计、 规范编制或者项目管理、 监理、 检测等服务的供应商， 不得再参与本项目投标（响应）。 投标函相关承诺要求内容。

8	本采购包专门面向中小企业采购	本采购包预留合同总额的 40% （或以上）专门面向中小企业采购。对于该预留份额部分，须由符合政策要求的中小企业承接。投标人可将满足预留部分金额的内容分包给一家或者多家中小企业，并在《分包意向协议》中载明分包承担主体、分包工作内容及金额，分包承担主体不得再次分包，投标时须提供《分包意向协议书》以及按规定填写《中小企业声明函》。若投标人为部分服务内容的供应商且为中小企业的，该部分内容无须分包。投标人与接受分包合同的中小企业之间不得存在直接控股、管理关系。（中小企业以投标人填写的《中小企业声明函》为判定标准，残疾人福利性单位以投标人填写的《残疾人福利性单位声明函》为判定标准，监狱企业须提供由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，否则不予认定。）。（2）由中小企业承担的内容需至少包括： 1. 可视化屏租赁服务； 2. 安全和密码资源池租赁服务； 3. 全厅 REDIS、CA 设备及证书和安全产品特征库升级授权租赁服务； 4. 安全基础设施租赁服务； 5. 广东省自然资源一体化管理与服务平台（国土空间基础信息平台）云盘。
---	----------------	---

表二符合性审查表：

采购包1（广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务））：

序号	评审点要求概况	评审点具体描述
1	投标有效期	符合投标有效期要求
2	投标保证金	投标保证金已按招标文件要求缴纳
3	投标文件按照招标文件规定要求签署、盖章	投标文件按照招标文件规定要求签署、盖章，包含：①投标函；②法定代表人证明书或法定代表人授权书；③开标一览表；④分项报价表
4	投标报价	投标报价未超项目预算（限价）
5	标注“★”的条款的满足情况	完全满足招标文件中标注“★”的条款
6	未出现有关法律、法规、规章或招标文件规定的属于投标无效的情形	未出现有关法律、法规、规章或招标文件规定的属于投标无效的情形

2.投标文件澄清

2.1对于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，评标委员会应当在评审过程中发起在线澄清，要求投标人针对价格或内容做出必要的澄清、说明或补正。代理机构可根据开标环节记录的授权代表人联系方式发送短信提醒或电话告知。

投标人需登录广东政府采购智慧云平台项目采购系统的等候大厅，在规定时间内完成澄清（响应），并加盖电子印章。

若因投标人联系方式错误未接收短信、未接听电话或超时未进行澄清（响应）造成的不利后果由供应商自行承担。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。

2.2评标委员会不接受投标人主动提出的澄清、说明或补正。

2.3评标委员会对投标人提交的澄清、说明或补正有疑问的，可以要求投标人进一步澄清、说明或补正。

3.详细评审

采购包1(广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）):

评审因素	评审标准
------	------

分值构成	商务部分 42.0分 技术部分 48.0分 报价得分 10.0分	
技术部分	带“▲”条款响应情况 (18.0分)	根据投标人对“第二章 采购需求”中带“▲”条款的响应情况进行评分： 投标人所投产品（需明确所投产品厂商和型号）每满足招标文件“第二章 采购需求”中带“▲”条款任一条要求的，得1分，最高得18分。注：1.如采购需求中有明确要求提供证明资料的，以采购需求中的要求为准；如采购需求中未明确要求提供证明资料的，以投标人响应情况为准。2.相关证明文件提供封面页及关键页，建议对所需证明的内容予以标注。
	统一运维管理方案需求响应1 (3.0分)	针对采购需求中的“4.3 运行维护服务”章节内容，根据供应商提供的统一运维管理方案需求响应进行评审，需包括：1.巡检和故障管理； 2.安全和问题管理； 3.变更管理。 每提供1项得1分，本项最高得3分。本项不得分的，统一运维管理方案需求响应2均不得分。
	统一运维管理方案需求响应2 (4.0分)	根据投标人提供的统一运维管理方案需求响应进行评审：1、内容完善，科学合理，可操作性强，能有效保障本项目实施，有利于实现项目效果的，得4分； 2、内容较完善，较科学合理，可操作性较强，能有效保障本项目实施，有利于实现项目效果的，得2分； 3、内容基本完善，基本科学合理，可操作性欠缺，能保障本项目实施，得1分； 4、不提供的不得分。
	业务系统运行维护服务方案1 (3.0分)	根据投标人提供的业务系统运行维护服务方案进行评审，需包括：1.各系统服务内容的梳理与分析 2.服务要求的解读与响应 3.针对性系统运维实施的具体方案制定 每提供1项得1分，本项最高得3分。本项不得分的，业务系统运行维护服务方案2均不得分。
	业务系统运行维护服务方案2 (5.0分)	根据投标人提供的业务系统运行维护服务方案进行评审：1、内容完善，科学合理，可操作性强，能有效保障本项目实施，有利于实现项目效果的，得5分； 2、内容较完善，较科学合理，可操作性较强，能有效保障本项目实施，有利于实现项目效果的，得3分； 3、内容基本完善，基本科学合理，可操作性欠缺，能保障本项目实施，得1分； 4、不提供的不得分。
	业务系统支撑环境运行维护服务方案1 (3.0分)	根据投标人提供的业务系统支撑环境运行维护服务方案进行评审，需包括：1.自然资源云专区数据库实例运维服务内容的梳理与分析 2.自然资源云专区基础组件运行维护服务内容的梳理与分析 3.运维技术保障方案 每提供1项得1分，本项最高得3分。本项不得分的，业务系统支撑环境运行维护服务方案2均不得分。
	业务系统支撑环境运行维护服务方案2 (4.0分)	根据投标人提供的业务系统支撑环境运行维护服务方案进行评审：1、内容完善，科学合理，可操作性强，能有效保障本项目实施，有利于实现项目效果的，得4分； 2、内容较完善，较科学合理，可操作性较强，能有效保障本项目实施，有利于实现项目效果的，得2分； 3、内容基本完善，基本科学合理，可操作性欠缺，能保障本项目实施，得1分； 4、不提供的不得分。

	基础设施运行维护方案1 (2.0分)	根据投标人提供的基础设施运行维护方案进行评审，需包括: 1.服务内容的全面梳理与分析 2.服务要求的解读与响应 每提供1项得1分，本项最高得2分。本项不得分的，基础设施运行维护方案2均不得分。
	基础设施运行维护方案2 (2.0分)	根据投标人提供的基础设施运行维护方案进行评审: 1、内容完善，科学合理，可操作性强，能有效保障本项目实施，有利于实现项目效果的，得2分； 2、内容较完善，较科学合理，可操作性较强，能有效保障本项目实施，有利于实现项目效果的，得1分； 3、内容基本完善，基本科学合理，可操作性欠缺，能保障本项目实施，得0.5分； 4、不提供的不得分。
	自然资源业务网网络平面运维服务方案1 (2.0分)	根据投标人提供的自然资源业务网网络平面运维服务方案进行评审，需包括: 1.服务内容的全面梳理与分析 2.服务要求的解读与响应 每提供1项得1分，本项最高得2分。本项不得分的，自然资源业务网网络平面运维服务方案2均不得分。
	自然资源业务网网络平面运维服务方案2 (2.0分)	根据投标人提供的自然资源业务网网络平面运维服务方案进行评审: 1、内容完善，科学合理，可操作性强，能有效保障本项目实施，有利于实现项目效果的，得2分； 2、内容较完善，较科学合理，可操作性较强，能有效保障本项目实施，有利于实现项目效果的，得1分； 3、内容基本完善，基本科学合理，可操作性欠缺，能保障本项目实施，得0.5分； 4、不提供的不得分。
	项目负责人 (3.0分)	投标人拟安排投入本项目的项目负责人（由主体投标方提供，1名，不得与其他岗位人员重复，否则不得分）： 1、学历专业方面：具有计算机类专业本科学历得0.5分，硕士研究生或以上学历，得1分； 2、资质证书方面：具有系统规划与管理师证书或信息系统项目管理师证书的，得1分； 3、工作经验方面：作为项目负责人（项目经理）具有运维相关项目管理经验的，每提供1个得0.5分，本小点最高得1分。本项最高得3分。注：①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则该小点不得分。②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。③项目经验需要提供合同关键页，并体现项目负责人（项目经理）姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则该小点不得分。④建议投标人在投标文件中明确注明项目负责人的所属人员，如项目涉及分包，项目负责人必须由主体投标方（即非分包承接商）的人员担任，否则不得分。

软件系统运维（安全）负责人 (2.0分)	投标人拟安排投入本项目的软件系统运维（安全）负责人（由主体投标方提供，1名，不得与其他岗位人员重复，否则不得分）： 1、学历专业方面：具有信息安全相关专业本科或以上学历的，得0.5分； 2、资质证书方面：具有信息安全工程师证书（计算机技术与软件专业技术资格），得0.5分； 3、工作经验方面：作为运维项目负责人或者专设的安全负责人，且具有安全运维相关项目管理经验（如项目中只明确一个负责人，但项目涉及安全内容，同样视为具备安全运维经验）的，每提供1个得0.5分，本小点最高得1分。本项最高得2分。注：①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则该小点不得分 ②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。③项目经验需要提供合同关键页，并体现运维安全负责人姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则该小点不得分。④建议投标人在投标文件中明确注明软件系统运维（安全）负责人的所属人员，如项目涉及分包，软件系统运维（安全）负责人必须由主体投标方（即非分包承接商）的人员担任，否则不得分。
软件系统运维（各业务子系统运维）负责人 (19.0分)	投标人拟安排投入本项目的软件系统运维（各业务子系统运维）负责人（由主体投标方提供，19名，不得与其他岗位人员重复，否则不得分）： 1.学历专业方面：具有计算机类或信息系统或电子信息类专业本科或以上学历的； 2.资质证书方面：具有系统规划与管理师或系统分析师或系统集成项目管理工程师（计算机技术与软件专业技术资格）的； 3.工作经验方面：具有信息系统运维相关项目经验的。以上三方面都满足的，每1人得1分；以上三方面满足其二的，每1人得0.5分；以上三方面满足其一的，每1人得0.2分；本项最高得19分。注：①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则视为该小点不满足。②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。③项目经验需要提供合同关键页，并体现该人员姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则视为该小点不满足。④建议投标人在投标文件中明确注明软件系统运维（各业务子系统运维）负责人的所属人员，如项目涉及分包，软件系统运维（各业务子系统运维）负责人必须由主体投标方（即非分包承接商）的人员担任，否则不得分。

商务部分	软件系统运维（业务系统支撑环境运维）负责人 (1.0分)	投标人拟安排投入本项目的软件系统运维（业务系统支撑环境运维）负责人（由主体投标方提供，1名，不得与其他岗位人员重复，否则不得分）： 1、学历专业方面：具有计算机类专业本科或以上学历的； 2、资质证书方面：具有系统集成项目管理工程师（计算机技术与软件专业技术资格）的； 3、工作经验方面：具有业务系统支撑环境（云专区）相关项目经验的。 以上三方面都满足的，得1分；以上三方面满足其二的，得0.5分；以上三方面满足其一的，得0.2分。本项最高得1分。注： ①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则视为该小点不满足。 ②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。 ③项目经验需要提供合同关键页，并体现该人员姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则视为该小点不满足。 ④建议投标人在投标文件中明确注明软件系统运维（业务系统支撑环境运维）负责人的所属人员，如项目涉及分包，软件系统运维（业务系统支撑环境运维）负责人必须由主体投标方（即非分包承接商）的人员担任，否则不得分。
	软件系统运维（业务系统支撑环境运维）云专区数据库运维工程师 (6.0分)	投标人拟安排投入本项目的软件系统运维（业务系统支撑环境运维）云专区数据库运维工程师（由主体投标方提供，6名，不得与其他岗位人员重复，否则不得分）： 1、学历专业方面：具有计算机类专业本科或以上学历的； 2、资质证书方面：具有数据库系统工程师证书（计算机技术与软件专业技术资格）的； 3、工作经验方面：具有系统运维或数据库相关项目经验的。 以上三方面都满足的，每1人得1分；以上三方面满足其二的，每1人得0.5分；以上三方面满足其一的，每1人得0.2分。本项最高得6分。注： ①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则视为该小点不满足。 ②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。 ③项目经验需要提供合同关键页，并体现该人员姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则视为该小点不满足。 ④建议投标人在投标文件中明确注明软件系统运维（业务系统支撑环境运维）云专区数据库运维工程师的所属人员，如项目涉及分包，软件系统运维（业务系统支撑环境运维）云专区数据库运维工程师必须由主体投标方（即非分包承接商）的人员担任，否则不得分。

软件系统运维（业务系统支撑环境运维）云专区基础组件运维工程师 (6.0分)	投标人拟安排投入本项目的软件系统运维（业务系统支撑环境运维）云专区基础组件运维工程师（由主体投标方提供，6名，不得与其他岗位人员重复，否则不得分）： 1、学历专业方面：具有计算机类或电子信息类专业本科或以上学历的； 2、资质证书方面：具有系统架构设计师或网络工程师证书（计算机技术与软件专业技术资格）的； 3、工作经验方面：具有云平台相关项目经验的。 以上三方面都满足的，每1人得1分；以上三方面满足其二，每1人得0.5分；以上三方面满足其一的，每1人得0.2分。本项最高得6分。 注： ①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则视为该小点不满足。 ②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。 ③项目经验需要提供合同关键页，并体现该人员姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则视为该小点不满足。 ④建议投标人在投标文件中明确注明软件系统运维（业务系统支撑环境运维）云专区基础组件运维工程师的所属人员，如项目涉及分包，软件系统运维（业务系统支撑环境运维）云专区基础组件运维工程师必须由主体投标方（即非分包承接商）的人员担任，否则不得分。
业务网络平面运维和基础设施运维工程师 (2.0分)	拟安排投入本项目的业务网络平面运维和基础设施运维工程师（由主体投标方提供，2名，不得与其他岗位人员重复，否则不得分）： 1. 学历专业方面：具有网络工程相关专业本科或以上学历的； 2. 资质证书方面：具有网络工程师证书（计算机技术与软件专业技术资格）的； 3. 工作经验方面：具有网络运维或基础设施运维相关项目经验的。 以上三方面都满足的，每1人得1分；以上三方面满足其二，每1人得0.5分；以上三方面满足其一，每1人得0.2分。本项最高得2分。 注： ①提供人员的资质证书复印件，学历的提供学历证书复印件（如为国(境)外学历学位证书须同时提供中文翻译，及教育部留学服务中心出具的国外学历学位认证书。）。否则视为该小点不满足。 ②提供投标文件递交截止前3个月中任意一个月供应商（含分支机构）为其缴纳的社保证明复印件（代缴个税税单，或参加社会保险（须至少体现养老保险）的《投保单》等证明均可）。否则该人员不得分。 ③项目经验需要提供合同关键页，并体现该人员姓名。如无法体现的，需提供相关说明材料（格式自拟）并加盖项目经验客户方公章。否则视为该小点不满足。 ④建议投标人在投标文件中明确注明业务网络平面运维和基础设施运维工程师的所属人员，如项目涉及分包，业务网络平面运维和基础设施运维工程师必须由主体投标方（即非分包承接商）的人员担任，否则不得分。
同类项目业绩 (3.0分)	2023年1月1日（以合同签订日期为准）以来，主体投标方承担过系统运维等相关项目，每个得0.5分，本项合计最高得3分。 注：业绩材料需提供合同及验收报告的复印件，并能反映建设内容、签署盖章、日期等关键内容，未提供不得分，相同业绩不重复计分。

异常低价审查	异常低价审查	根据《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）等相关规定，政府采购评审中出现下列情形之一的，评审委员会应当启动异常低价投标（响应）审查程序：（1）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值65%的，即投标（响应）报价 $<$ 全部通过符合性审查供应商投标（响应）报价平均值 $\times 65\%$ 。（2）投标（响应）报价低于通过符合性审查且报价次低供应商投标（响应）报价65%的，即投标（响应）报价 $<$ 通过符合性审查且报价次低供应商投标（响应）报价 $\times 65\%$ 。（3）投标（响应）报价低于最高限价65%的，即投标（响应）报价 $<$ 最高限价 $\times 65\%$ 。（4）其他评审委员会认为供应商报价过低，有可能影响产品质量或者不能诚信履约的情形。评审委员会启动异常低价投标（响应）审查后，应当要求相关供应商在评审现场合理的时间内提供书面说明及必要的证明材料，对投标（响应）价格作出解释。
投标报价	投标报价得分 (10.0分)	投标报价得分=（评标基准价/投标报价） $\times$ 价格分值【注：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。】最低报价不是中标的唯一依据。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。

4.汇总、排序

采购包1:

评标结果按评审后总得分由高到低顺序排列。总得分相同的按投标报价由低到高顺序排列。得分且投标报价相同的，由评委会采取随机抽取的方式确定。排名第一的投标供应商为第一中标候选人，排名第二的投标供应商为第二中标候选人（提供相同品牌产品（非单一产品采购，以核心产品为准。多个核心产品的，有一种产品品牌相同，即视为提供相同品牌产品），评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定，其他同品牌投标人不作为中标候选人）。

5.中标价的确定

除了按第四章第一点第7条修正并经投标人确认的投标报价作为中标价外，中标价以开标时公开唱标价为准。

6.其他无效投标的情形:

(1)评标期间，投标人没有按评标委员会的要求提交法定代表人或其委托代理人签字的澄清、说明、补正或改变了投标文件的实质性内容的。

(2)投标文件提供虚假材料的。

(3)投标人以他人名义投标、串通投标、以行贿手段谋取中标或者以其他弄虚作假方式投标的。

(4)投标人对采购人、采购代理机构、评标委员会及其工作人员施加影响，有碍招标公平、公正的。

(5)投标文件含有采购人不能接受的附加条件的。

(6)法律、法规和招标文件规定的其他无效情形。

合同编号：

省级政务信息化项目
合同书

项 目 名 称：广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）

委托方（甲方）：广东省国土资源技术中心

受托方（乙方）：

签 订 日 期：__年__月

签 订 地 点：__省__市__区

广东省政务服务和数据管理局印制

填 写 说 明

一、本合同为广东省政务服务和数据管理局印制的项目服务合同示范文本，省各有关单位可参照使用。

二、本合同书适用于一方当事人（受托方）为另一方（委托方）提供省级政务信息化服务（含软件开发服务、基础设施服务、运维服务）所订立的合同。

三、签约一方为多个当事人的，可按各自在合同关系中的作用等，在“委托方”、“受托方”项下（增页）分别排列为共同委托人或共同受托人。

四、本合同书未尽事项，可由当事人附页另行约定，并作为本合同的组成部分。

五、当事人使用本合同书时约定无需填写的条款，应在该条款处注明“无”等字样。

第一章总则

1. 相关术语的定义和解释

1.1.1. 定义

1.1.1.1. 本项目：广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）（采购项目编号：_____）。

1.1.1.2. 委托方/甲方：本项目采购人。

1.1.1.3. 受托方/乙方：本项目成交供应商。

1.1.1.4. 咨询、监理单位：受甲方委托对本项目进行第三方咨询、监理的单位。

1.1.1.5. 测试、测评单位：受甲方或乙方委托对本项目进行第三方测试、安全等保测评等服务的单位。

1.1.1.6. 省各有关单位：经广东省机构编制委员会批准设立的广东省行政事业单位，主要包括省政府办公厅、省政府组成部门、省政府直属特设机构、省政府直属机构、部门管理机构、其他机构、省政府直属事业单位、其他。

1.1.1.7. 适用法律：指所有适用的中华人民共和国法律、法规、部门规章、地方性法规、司法解释、政府部门颁布的标准、规范或其他适用的强制性要求、有法律约束力的规范性文件等。除非另有特别约定或文意另有所指，本合同中提及的“法律”均包括适用法律的全部定义内容。

1.1.1.8. 法律变更：指在生效后颁布、修订、废止或重新解释的任何适用法律导致甲方或乙方在本合同项下的权利义务发生实质性变化。

1.1.1.9. 批准：指为了使乙方能够履行其在本合同项下的义务和行使其在本合同项下的权利，乙方必须从甲方或省各有关单位依法获得的为乙方的建设、运营、运维所需要的任何许可、同意、授权等。

1.1.1.10. 生效日：指本合同甲乙双方盖章并由双方法定代表人或授权代表人签字之日。如依照适用法律需要履行审批程序的，则在有权部门审批后生效。

1.1.1.11. 服务实施：指乙方根据本合同开展服务实施准备、执行、收尾等为实现服务交付开展的工作。

1.1.1.12. 服务交付：指乙方根据本合同提交交付验收申请，经甲方组织验收后确认服务交付的过程。

1.1.1.13. 服务运行：指自服务交付验收完成时起至合同约定期限届满时止，乙方按本合同提供的服务。

1.1.1.14. 交付验收：指对服务提供方拟交付使用的软件系统或基础设施进行验收。

1.1.1.15. 阶段性服务确认：指服务提供方按项目合同要求，完成某一时间段服务，对服务成果进行确认，适用于基础设施服务项目、运维服务项目。

1.1.1.16. 最终验收：对项目整体服务的验收。

1.1.1.17. 服务正式上线：指乙方提供的服务经交付验收合格后，甲方确认服务正式上线，作为服务上线运行的标志。

1.1.1.18. 服务期限：指本项目周期、期限。

1.1.1.19. 粤复用：是指广东数字政府应用超市，汇聚各级政府部门数字政府应用、服务商产品、组件等资源，以“快速、可靠、低成本”为原则，推动“一地创新，各地复用”，实现数字政府建设模式变革。

1.1.1.20. 复用推广：是指在“粤复用”平台上架的应用、产品和组件等资源在全省政府部门、事业单位和国有企业进行复用推广。

1.1.1.21. 其他在本合同及相关附件中涉及的有关名词和技术术语，其定义和解释如下：

(1) _____；

(2) _____。

1.2. 解释

1.2.1. “工作日”是指国家所规定的节假日之外的所有的工作日，凡本合同所约定的工作日均指工作日，未指明工作日的日期指自然顺延的日期。

1.2.2. 所指的日、月和年均指公历的日、月和年，其中一年以三百六十五日计，一个月以三十日计。

1.2.3. “不可抗力”是指任何一方由于出现不可抗力事件使该方无法全部或部分履行其本合同项下的义务致使合同目的不能实现时，该方应有权中止履行本合同项下的义务，但应及时通知对方，以减轻可能给对方造成的损失，并应在合理期限内向对方提供不可抗力的证明。

1.2.4. “元”是指人民币元。

1.2.5. 条款或附件：指本合同的条款或附件。

1.2.6. 除非本合同另有明确约定，“包括”指包括但不限于；除本合同另有明确约定，“以上”、“以下”、“以内”或“内”均含本数，“超过

”、“以外”不含本数。

2. 声明和保证

2.1. 甲方的声明和保证

2.1.1. 在本合同生效日前已获得了签订本合同所必需的授权，有权签署本合同。

2.1.2. 甲方应保证对向乙方提供的与本项目相关的材料、信息或数据的准确性、完整性或适宜性负责；甲方对向乙方提供的其他材料、信息或数据的准确性、完整性或适宜性，未作出任何保证。

2.1.3. 如果甲方的保证被证明在做出时存在不实或不能兑现，对乙方依本合同享有权利或承担义务造成实质性影响时，乙方有权提前终止本合同。本合同各附件也随之自动终止。

2.2. 乙方的声明和保证

2.2.1. 乙方是依据中国法律正式成立的企业法人或具有法人资格的事业单位和社会团体，具有签署和履行本合同的法人资格及履约能力。

2.2.2. 乙方为签署本合同已经依据适用法律及公司章程之规定完成所有必要的公司内部行为，其有权签署本合同并履行本合同项下的义务。

2.2.3. 乙方应保证向甲方提供本项目服务内容前，已达到提供相应服务的能力，包括符合国家、广东省相关标准规范或行业标准规范。

2.2.4. 如果乙方的保证被证明在做出时存在不实或不能兑现，对甲方依本合同享有权利或承担义务造成实质性影响时，甲方有权提前终止本合同，并保留追究损失的权利。本合同各附件也随之自动终止。

第二章合同主体的权利和义务

3. 甲方

3.1. 权利

3.1.1. 甲方有自行或委托第三方机构，对乙方提供的本项目的服务进行监管的权利。

3.1.2. 甲方有自行或委托第三方机构，对乙方的建设、运维、管理、安全、质量、服务状况进行定期评估考核的权利。

3.1.3. 乙方因自身原因导致合同无法继续履行，则视为违约，甲方有权单方解除合同，并向乙方追偿损失。

3.1.4. 如因乙方原因导致甲方被行政处分或行政处罚，甲方保留向乙方追究法律责任、经济责任的权利。

3.1.5. 法律、法规授予甲方的其他权利。

3.2. 义务

3.2.1. 依据乙方的书面申请，在不影响正常工作的前提下协助乙方及时获得本项目需要的合理、合法的条件，包括但不限于成立项目协调小组或安排专人负责配合乙方开展服务，协调乙方与相关单位的工作关系，保障项目顺利实施和运营维护以及提供本项目所需水、电、服务场地、信息和数据等相关事宜；对委托给乙方运维的政务信息系统所涉及的知识产权取得合法授权（如有）。

3.2.2. 甲方应依照合同要求向乙方提供技术服务所必需的信息、数据、资料，并负责为乙方提供必要的设备、工作场地、后勤设施等。如因甲方未能按时提供工作条件或技术资料，或甲方未及时协调需其他相关方配合的资源，经甲乙双方协商可顺延服务工作的完成期限。

3.2.3. 甲方应在项目小组指派一名甲方人员作为项目负责人，负责对乙方服务进行协调、监督，项目负责人应定期向甲方汇报，与乙方项目负责人沟通，并负责本合同项下服务和/或可交付成果物的验收组织工作。如乙方提供的服务达不到甲方要求的，甲方应及时将不符合要求的内容和原因通知乙方。

3.2.4. 甲方应及时组织验收，对乙方提交的符合本合同约定的服务成果进行书面确认。

3.2.5. 按照本合同的约定向乙方支付合同金额。

3.2.6. 及时审核并确认乙方提交的服务成果、进度报告等。

3.2.7. 若甲方在其他合同中为本项目指定监理单位，甲方应当将授予监理单位的监理权利及时通知乙方。

3.2.8. 法律、法规规定的以及本合同项下的其他义务。

4. 乙方

4.1. 权利

4.1.1. 要求甲方按本合同的约定支付合同金额的权利。

4.1.2. 如果因不可归责于乙方的原因导致乙方不能履约的，则乙方有权和甲方就有关事宜进行沟通，如经甲方确认确属不可归责于乙方的原因，且乙方已为避免此种情形采取必要的措施，则甲方出具相应的书面文件，确认不得以此作为对乙方考核不达标的依据，并不得追究乙方的违

约责任。

4.1.3.法律、法规规定以及本合同规定的其他权利。

4.2. 义务

4.2.1.按照本合同约定（包括进度、质量、安全标准）完成本项目。

4.2.2.接受甲方或其指定的第三方机构对本项目的监管、评估考核等。

4.2.3.服务期内，如遇国家法律、法规及相关政策发生重大变化，对本合同的履行造成实质性的影响，乙方应积极与甲方协商解决，并采取合理措施避免各方的损失扩大。

4.2.4.如政府审计部门或政府审计部门委托的第三方审计单位需对涉及本合同的事项进行审计时，乙方应按照政府审计有关法律法规和政策要求，支持、协助审计部门或其委托的跟踪审计单位开展工作。

4.2.5. 乙方应加强项目相关人员管理。向甲方书面提交本合同项目具体的人力资源计划及岗位职责手册（包括但不限于：本合同项目的管理、开发、运营、运维等服务人员的名单、岗位职责、组织架构等），如有变化乙方应及时更新，核心骨干人员（一般为项目经理、技术负责人）变化须应提前征得甲方事先同意，甲方认为乙方派出的人员不足以按期保质完成服务任务，乙方应按甲方要求更换，更换人员须经过甲方面试同意。如仍不能符合项目服务质量要求，采购人有权责令停止服务并整改或解除合同，乙方应对由此造成的损失负责。与本项目有关的规章制度以及服务过程有关资料，乙方应书面报甲方备案，并接受甲方定期不定期的检查。应加强对驻场人员管理，遵守甲方工作管理要求，接受工作指导和统一安排。

4.2.6. 乙方应保证所提供的产品或服务没有侵害任何第三方的知识产权或其他正当权益。如有第三方指控甲方接受乙方提供的产品或服务侵犯了该方的知识产权或其他合法权利，乙方应自费就上述指控为甲方辩护或进行妥善处理，并承担给甲方及第三方造成的一切损失（包括但不限于赔偿金、律师费、诉讼费等）。如乙方不为甲方辩护或不进行妥善处理，甲方可自行处理，对于甲方与第三方达成的和解协议或法院、仲裁机构作出的生效法律文书确定由甲方承担的责任和费用，及甲方自行处理所支出的合理费用（包括但不限于律师费、案件受理费、执行费、差旅费等），乙方同意全部承担，甲方有权在应付乙方的合同款项中直接扣减相应金额或另行向乙方进行追偿。

4.2.7.合同履行期内，如乙方的股东拟转让股权的，乙方应按《公司法》等法律法规及《公司章程》履行相应的决策、审批程序，并及时向甲方报备。

4.2.8.合同履行期限届满后，或者按照本合同约定需要终止或解除合同的，乙方应配合甲方做好与项目相关的数据迁移、资料移交等工作。

4.2.9.若甲方在其他合同中为本项目指定咨询、监理单位，乙方应无条件接受甲方或甲方指定的咨询、监理单位的统一管理和监督检查，并按要求完成相关配合工作。

4.2.10.若甲方在其他合同中为本项目指定第三方验收测评机构，测评内容包括但不限于系统规模（功能点评估）、功能、性能、安全性、可靠性、易用性、维护性、可移植性等，乙方应无条件配合完成相关工作。

4.2.11. 乙方应对其履行本合同所雇佣、安排的全部人员的安全事故承担责任。由于乙方或乙方人员原因在甲方办公场所内及其毗邻造成的第三者人身伤亡和财产损失，由乙方负责赔偿，若造成甲方实际损失的，甲方有权向乙方全额追索。

4.2.12. 乙方须依据系统工程要求开展工作，按甲方要求提交系统工程设计书和系统工程验收报告，指派项目技术负责人并按甲方要求接受相关的系统工程能力考核。

4.2.13.涉及定制软件开发的服务内容，乙方应按甲方要求交付源代码。

4.2.14. 乙方须按甲方要求移交系统超级管理员和其他重要权限。

4.2.15. 乙方按甲方要求，配合完成本项目关联系统的数据资产、数字化资产建档建卡，包括但不限于：系统登记、资产清查盘点、建立并完善资产信息卡等工作。具体建档建卡要素和格式须符合财政部《关于加强行政事业单位数据资产管理的通知》（财资〔2024〕1号）、《固定资产等资产基础分类与代码》（GB/T 14885-2022）等国家和广东省相关政策，以及甲方内控制度的要求。乙方需保证其交付工作即数据资产信息的齐全性、准确性和真实性。

4.2.16. 乙方须按甲方制定的项目质量管理要求开展服务，无条件接受甲方对项目质量管理要求落实情况的监督考核。包括但不限于：根据甲方提出的项目需重点解决问题清单提供解决方案，在项目实施过程中将问题予以解决，确保项目服务质量；根据甲方提出的项目管理制度清单，编制相应的项目管理制度文件，进一步规范项目实施过程；根据甲方提出服务团队岗位职责清单，制定岗位职责手册，定岗定人，确保各核心岗位均指派能胜任的专人提供服务。

4.2.17. 乙方应当按照合同约定履行义务，完成中标项目。除甲方在采购文件明确允许以分包形式履行，且乙方在投标环节已签订分包意向协议的服务内容外，乙方不得将合同服务内容以任何形式进行分包，不得向他人转让中标项目，也不得将中标项目肢解后分别向他人转让。

4.2.18本项目按照《政府采购促进中小企业发展管理办法》要求，部分面向中小企业采购，乙方应按招标文件的要求和投标文件的分包意向协议书，将以下非主体内容进行分包： 分包给 ，分包金额为 （¥ ），乙方须在本合同签订5个工作日内与分包商签订合同，确保资金使用符合上述分包内容，并向甲方报备合同原件1份，否则视乙方为本合同违约。乙方与分包商签订的合同应明确不得再次转包和分包所承担的工作内容。

4.2.19.在项目最终验收前，乙方须提交分包商履约情况报告、合同款项支付情况说明及银行付款记录。

4.2.20.根据乙方的投标文件，服务内容分包不代表解除或减免乙方在本项目下的任何义务，乙方应对上述分包商和其聘用的人员履行本合同的情况以及任何作为或不作为向甲方承担连带责任。

4.2.21.法律、法规规定的以及本合同项下的其他义务。

5. 其他相关方（若有，如用户单位）

5.1. 权利

根据项目需要，甲方将部分以下权利授予相关方：

- (1) _____； (2) _____；
- (3) _____； (4) _____；
- (5) _____；
- (6) _____。

5.2. 义务

伴随甲方授予的上述权利，相关方需履行以下义务：

- (1) _____； (2) _____； (3) _____；
- _____； (4) _____； (5) _____；
- _____；
- (6) _____。

第三章 服务内容及服务期限

6. 服务内容

本项目包括服务内容，包括：

- (1) 基础设施服务：包括可视化屏租赁、安全和密码资源池租赁、全厅REDIS租赁、CA设备及证书和安全产品特征库升级授权租赁服务、安全基础设施租赁；
- (2) 成品软件租赁服务：广东省自然资源一体化管理与服务平台（国土空间基础信息平台）云盘租赁；
- (3) 运行维护服务：包括基础设施运维服务：省自然资源厅及广东省国土资源技术中心各类基础设施的运行维护服务；软件系统运维服务：一是业务系统运行维护服务，包括广东省自然资源一体化数据库（自然资源三维时空数据库）等8个应用的运维服务；二是业务系统支撑环境运行维护服务，包括自然资源云专区基础组件运行维护服务和自然资源云专区数据库实例运维服务；其他运维服务：广东省自然资源业务网网络平面运维服务。

其他详细内容见附件。

7. 服务期限

本项目服务期限适用模式详见下表。

序号	大类	小类	建设内容	建设内容	服务期限采用模式
1	基础设施服务	专业基础设施服务	可视化屏租赁服务	/	第（1）种模式
2			安全和密码资源池租赁服务	/	第（1）种模式
3			全厅REDIS租赁服务	/	第（1）种模式
4			CA设备及证书租赁服务	/	第（1）种模式
5			安全产品特征库升级授权租赁服务	/	第（1）种模式
6			安全基础设施租赁服务	/	第（1）种模式
7	软件开发服务	成品软件租赁服务（许可）服务	广东省自然资源一体化管理与服务平台（国土空间基础信息平台）云盘	/	第（1）种模式
8	运行维护服务	基础设施运行维护服务	基础设施运行维护服务	/	第（1）种模式
9		软件系统运行维护服务	业务系统运行维护服务	广东省自然资源一体化数据库（自然资源三维时空数据库）运行维护服务	第（2）种模式
10				广东省自然资源一体化管理与服务平台（国土空间基础信息平台）运行维护服务	第（2）种模式
11				广东省自然资源和不动产登记综合应用运行维护服务	第（2）种模式
12				广东省国土空间用途管制综合应用运行维护服务	第（2）种模式
13				广东省自然资源市场与资产监管综合应用运行维护服务	第（2）种模式
14				广东省测绘地理信息管理综合应用运行维护服务	第（2）种模式
15				广东省自然资源厅城市地质信息管理服务平台运行维护服务	第（1）种模式
16				广东省国土资源技术中心政务服务综合保障子系统运行维护服务	第（1）种模式
17			业务系统支撑环境运行维护服务	自然资源云专区数据库实例运维服务	第（2）种模式
18				自然资源云专区基础组件运行维护服务	第（2）种模式
19		其他运行维护服务	广东省自然资源业务网（业务网平面）网络平面运维服务	/	第（1）种模式

（1）第1种模式：以采购人确认的服务启动报审备案时间为服务起始时间，服务期为12个月。服务起始时间不晚于2026年10月1日。

(2) 第2种模式：自2027年4月27日开始，至2027年10月27日止，共6个月。其中，一体化平台中云GIS模块的运行维护周期按第1种模式。

第四章服务实施和验收

8. 项目安全防护

8.1. 本项目服务实施期间，乙方应严格遵守国家相关安全规定。若因乙方原因出现任何安全问题，乙方应承担全部责任。

8.2. 甲方有权聘请第三方测评公司对乙方提供的信息系统进行安全等级保护测评，乙方应予以配合，确保其所提供的产品或服务满足公安部信息系统安全等保-级的要求。

8.3 未经甲方同意，乙方不得擅自调整本项目所涉及系统功能，或实施与其他业务系统对接等工作。

9. 项目进度保障

9.1. 乙方提交启动实施报审备案的同时向甲方提交一份本项目详细的《服务实施方案》（含《项目进度计划》、《里程碑计划》）供甲方审核，经甲方审核通过后，乙方应严格按照《服务实施方案》中规定的进度要求进行交付，实际交付验收合格时间以甲方出具验收报告的时间为准。

9.2. 项目进度计划可以按照月/周/日不同层级来进行细化。月度进度计划需要细化各个里程碑节点完成所涉及的全部工作内容和时间计划。周计划与日计划是月进度计划的具体工作实现。

9.3. 乙方应严格按照《服务实施方案》所规定的进度计划，选取提交定期报告（选取以下一种或多种方式），并于每月第3日前向甲方及监理单位提交《月度进度计划报告》，详细说明如下事项：

- (1) 当月项目目标计划；
- (2) 当月里程碑事件完成情况；
- (3) 存在的问题及解决建议，包含与进度计划的差异、原因分析及正在采取的纠正措施；
- (4) 统计分析，包含当月计划完成的服务事项及整体完成比例、预计本月完成的建设情况及预计建设时间等。
- (5) 进度变更（必须甲乙双方书面确认）。

9.4. 交付延误

如果乙方在项目实施过程中，由于不可抗力、政策调整、甲方需求变化、技术更新等客观原因导致交付时间不能满足本合同约定的进度要求，按照有利于项目成功的原则，乙方应立即通知甲方，并就变更背景、变更依据、相应的变更控制措施以及变更影响评估提出进度变更申请，提交第三方监理审核、甲方审批后执行变更。

9.5. 乙方发出上述通知并不能免除其在本合同中的任何义务。如果乙方提出或实施的补救措施不能解决逾期的延误，甲方可要求乙方采取甲方认为必要的其他措施以达到进度计划的要求，但甲方可根据迟延的客观原因及乙方的书面申请而给予乙方一定的宽限期限。

10. 项目质量保障

10.1. 乙方提供的服务应满足本合同约定的项目质量指标，包括项目过程质量指标、项目成果质量指标等。

10.2. 乙方在项目执行过程中应制定质量改进计划。质量改进计划的制定应以下三个步骤进行：

- (1) 明确问题。分析现状，找出项目存在的质量问题，包括确认质量问题，收集相关的质量数据；
- (2) 问题分析。分析产生项目质量问题的各种原因和影响因素，找出可能的影响因素并验证，比较并选择主要的、直接的影响因素；
- (3) 制定问题改进计划。针对质量问题的主要因素，制定措施，提出问题处理计划，包括问题解决方案，问题处理所需的资源需求等。

10.3. 质量改进计划制定后，乙方应按照既定的计划，根据国家、广东省、行业相关的规范标准，制定项目的质量改进目标，明确改进的质量指标，设定质量测量的方法和时间，确定质量改进的岗位责任安排等，通过质量管理规范指导项目实施，并对发现的质量问题逐个进行处理。

10.4. 质量改进计划执行过程中或执行之后，乙方应对照质量改进计划，及时检查质量改进执行情况和效果，并与质量目标、质量管理指标进行对比分析，明确是否符合质量改进的预期目标，及时发现计划实施过程中的存在的问题，总结经验。质量改进检查包括乙方自查、第三方监理和甲方的定期巡查、不定期抽查以及第三方机构测评检查三种方式。各类项目应依据项目特点选择相应的质量检查方式。

10.5. 乙方应根据质量检查的结果对项目质量问题及时整改处理，同时对质量管理的运行情况进行总结与分析，对成功的经验加以肯定，并予以标准化，对失败的教训进行总结，引起重视。对未能及时处理解决的问题，需将其作为下一管理循环的质量改进目标。项目质量问题解决完成后，需对实施效果进行评估和记录。若采取的整改措施未达到预期效果，应重新制定解决措施，直至达到预期效果。

10.6.在不影响乙方履行本合同项下义务的情况下，甲方有权在工作时间内对乙方履约情况进行检查，以保证乙方项目的任何部分均符合本合同的要求。乙方须对此项检查予以协助。

10.7.甲方有材料证明乙方服务实施过程中与本协议所规定的或其他相关部门所规定的质量或安全要求严重不符时，甲方有权立即通知乙方，乙方应按要求进行整改。若乙方在收到甲方书面通知后十个工作日内未整改，则甲方有权自己进行或委托第三方进行必要的纠正，由此产生的一切风险与费用由乙方承担。

10.8.除本协议另有规定外，对乙方提交的质量保证与质量控制方案，甲方的任何作为或不作为，均不会：

- （1）减轻或影响乙方遵守本协议或法律所要求的与质量保证有关的义务或责任；
- （2）被视为甲方应对质量保证与质量控制方案承担任何责任。

10.9 项目存在运维服务的，乙方应在运维服务期内，收到甲方通知的小时内组织人员予以解决，相关费用由乙方承担。如乙方未能完成上述约定的质保义务，甲方可自行委托第三方进行维护，所产生的全部费用和损失由乙方承担。

11. 项目管理要求

11.1.甲方为服务项目业主方，用户方根据项目实际情况由甲方指定，用户方有参与对乙方相关服务管理、评价的权利。乙方应及时响应甲方和用户方的服务要求。

11.2.甲方有权随时自己或委托监理单位检查乙方的服务是否符合本合同的要求。

- （1）若发现任何部分不符合要求，甲方有权通知乙方，指出不符合规定之处。
- （2）若乙方对甲方根据上述第（1）款所发出的通知有异议，则须于接到甲方通知后的七日内将其异议及理由书面告知甲方，否则应提出整改方案和措施报甲方批准后进行整改。甲方与乙方须尽合理努力以求解决此项事宜。若该问题在乙方收到甲方通知后十四日内不能得到解决，则依据争议解决程序就该事宜进行解决。

11.3.甲方是否监督、检验本项目均不能减免乙方在本合同下的任何义务、责任。

12. 项目变更

甲方、乙方均可提出变更请求。项目变更时为确保效率，如无涉及项目合同金额变动且甲方认为没有必要的情形，服务项目可按照双方书面确认的往来文件立即实施。如涉及项目合同金额变动或甲方认为有必要的情形，乙方必须按甲方要求完成变更申请流程工作后由双方签订补充协议。

12.1.甲方要求的变更

12.1.1.甲方的变更通知

甲方认为需要对服务要求进行变更，应书面通知乙方。

12.1.2.乙方对变更的回复

乙方在收到甲方要求变更的通知后的七日（或甲方同意的延长期限）内，须就变更向甲方作出书面答复。如果乙方未按规定的时间回复，则视为乙方已接受了变更。

12.1.3.甲方的答复

在收到乙方对变更的回复后七日内，甲方须以书面方式确认乙方对变更的回复中所包含的事项，若甲方以书面形式表明不同意乙方对变更的回复，并列明不同意的具体事由，在此情况下，该变更将依照争议解决程序的规定进行解决。

12.2. 乙方要求的变更

12.2.1. 乙方的变更通知

乙方在本合同履行期间，认为需要对服务实施进行变更（但乙方提出的变更要求，必须是出于优化方案、节省开支等合理或经济性考虑），应书面通知甲方并经甲方书面同意后方可实施，否则不得变更。

12.2.2. 甲方的回复

甲方在收到乙方要求变更的通知后的十个工作日内，须就变更向乙方作出书面回复，否则视为不同意。

12.2.3. 乙方要求的变更的实施

当甲方书面同意乙方要求的变更时，本合同应视为在当日作出了变更，双方须遵守其各自在变更后的本合同项下的义务。当甲方不同意乙方要求的变更时，双方按原约定执行。

12.3. 变更的实施

在变更被甲方确认之后：本合同被视为在甲方确认当日作出了变更，且甲方与乙方须遵守在变更后的本合同项下所应承担的义务；乙方须按甲方变更通知所要求的方式或前述争议解决结果，实施该项变更；除本合同另有明确约定外，甲方的变更引起的工作量增减的，增减工作量由乙方提出，报经甲方审核通过后，由乙方负责实施。

12.4. 减轻损失的义务

12.4.1. 乙方应始终尽一切合理的努力，以减轻或降低乙方和甲方因变更而花费的支出和发生的损失。

12.4.2. 因变更所致的延误。因甲方要求的变更而导致竣工验收日的迟延，乙方有权向甲方申请给予相应的宽展期，经甲方盖章确认后生效。

13. 服务验收

乙方应按本合同约定及时申请验收，甲方收到乙方验收申请后，应及时审核，并在审核通过后按本合同约定及时组织验收，并出具验收报告。详细要求以附件 2 验收要求为准。

第五章合同金额与结算方式

14. 合同金额

合同总金额为（大写）：人民币_____元整(¥_____元)，其中涉及软件开发 服务金额为人民币_____元整(¥_____元)，基础设施服务金额为人民币_____元整(¥_____元)，运行维护服务金额为人民币_____元整(¥_____元)，本合同总金额为乙方按照合同约定完成合同全部义务后所适用的含税总价格。

15. 结算方式

15.1. 费用结算方式

15.1.1. 本项目计划分5期支付，具体支付方式和时间如下：

第1期：本项目签订合同生效后，乙方书面提出支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票，甲方确认后在10个工作日内启动进度款支付流程，支付合同总额的30%。

第2期：2026年11月25日前，采购人对截至2026年10月31日的项目实施成果进行阶段性考核，根据考核情况对投标人的服务质量打分，并根据评价结果确定项目进度款支付金额。中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的10%。

第3期：2027年3月30日前，采购人对2026年11月至2027年3月的项目实施成果进行阶段性考核，根据考核情况对投标人的服务质量打分，并根据评价结果确定项目进度款支付金额。中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的20%。

第4期：2027年6月30日前，采购人对2027年4月至2027年6月的项目实施成果进行阶段性考核，根据考核情况对投标人的服务质量打分，并根据评价结果确定项目进度款支付金额。中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付合同总额的20%。

第5期：项目最终验收通过后，采购人根据考核情况对中标人的服务质量打分，并根据评价结果、实际服务期确定项目尾款支付金额。中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后在10个工作日内启动进度款支付流程，支付2027年度应付款项的20%。

15.1.2. 对于满足合同约定支付条件的，甲方应当自收到发票后10个工作日内将资金支付到合同约定的乙方账户，不得以机构变动、人员更替、政策调整等为由延迟付款，不得将采购文件和合同中未规定的义务作为向乙方付款的条件。

15.1.3. 如乙方未按照约定提供上述任一所需文件，则甲方有权顺延付款时间且不承担违约责任，同时乙方应履行义务的期限不予顺延。

15.2. 乙方账号信息

开户名称：

开户银行：

银行账号：

甲方向上述账户汇出款项后，即视为甲方已履行付款义务，在汇款过程中因乙方账户原因（包括但不限于账号被注销、被冻结等）导致其无

法收取款项的，由乙方承担相应后果。甲方有权直接在应付款项中扣除乙方应承担的违约金或赔偿金等对应款项。

15.3. 其他

除本合同明确约定的费用外，甲方无需对乙方支付任何额外费用和承担任何额外义务。在实际合同履行过程中，如果乙方未完全履行合同义务或履行的合同义务不符合约定的，则未履行或履行不符合合同约定的内容所对应的价款由甲方直接从上述约定的合同金额中扣除。

第六章不可抗力及法律变更

16. 不可抗力事件

不可抗力指任何一方无法预见、控制且经合理努力仍无法避免或克服的、导致其无法履行合同项下的义务的情形，包括但不限于：台风、地震、洪水等自然灾害；战争、罢工、骚乱等社会异常现象；征收征用等政府行为；以及甲乙双方不能合理预见和控制的任何其他客观情形。

17. 不可抗力事件的认定和评估

17.1. 认定和评估

17.1.1.受到不可抗力事件影响的一方应在不可抗力事件发生后七日内书面通知另一方，详细描述不可抗力的发生情况、必要的证明文件和可能导致的后果，并及时采取措施减少损失范围。

17.1.2. 甲方组织双方协商，评估和认定不可抗力。

17.2. 例外情况

17.2.1. 适用于乙方的例外情况

乙方无权将下述情况视作不可抗力事件而终止、中止履行本合同或不完全履行本合同项下义务：

- （1）其他与乙方建立合同关系的第三方在履行合同方面发生延误；
- （2）乙方提供服务的设施发生故障或正常磨损。

17.2.2. 适用于甲方的例外情况

甲方无权将下述情况视作不可抗力事件而终止、中止履行或不完全履行本合同项下义务：

甲方因机构改革发生变更。

18. 不可抗力事件发生期间各方权利和义务

18.1. 权利

18.1.1. 甲方有认定不可抗力事件对本合同影响的权利。

18.1.2. 乙方有权要求甲方按合同约定计量支付不可抗力事件发生前的合同金额。

18.2. 义务

18.2.1.受到不可抗力事件影响的一方按合同约定时限通知另一方。

18.2.2.双方均应采取合理措施尽量避免和减少损失的扩大。

18.2.3.声称不可抗力的一方在不可抗力消除之后应尽快恢复履行本合同项下的义务。

19. 不可抗力事件的处理

19.1.发生不可抗力时，双方应各自承担由于不可抗力对其造成的损失。双方应协商采取合理的补救措施尽量减少不可抗力给各方带来的损失。

19.2.不可抗力发生前已发生的合同金额应当按照合同约定进行计量支付。

19.3. 当不可抗力事件阻止一方履行其义务的时间持续九十日以上时，双方应协商决定继续履行本合同的条件或者终止本合同。如果自不可抗力发生后一百八十日之内双方不能就继续履行的条件或终止本合同达成一致意见，任何一方有权给予另一方书面通知后立即终止本合同。

第七章合同解除

20. 合同解除的事由

20.1.甲方或乙方在本合同中的声明或保证在被证实存在虚假或未兑现，严重影响其履约能力。

20.2.出现本合同约定的导致合同终止情形的。

20.3.发生其他导致本合同无法继续履行情形的。

21. 合同解除程序

21.1. 发出终止意向通知

21.1.1. 甲方发出的终止

下述任一行为发生时，甲方有权立即发出终止意向通知：

- （1）乙方在本合同中的声明或保证在被证实存在虚假或未兑现，严重影响其履约能力；
- （2）乙方出现本合同约定的导致合同终止情形的；
- （3）乙方被依法吊销营业执照、责令停业、清算或破产；
- （4）乙方未按《服务实施方案》时间节点完成本合同项下工作，逾期超过 30 日的；
- （5）乙方发生累计两次或以上违约行为；
- （6）乙方履行义务不符合约定，经甲方提出后合理期限内仍未改正的；
- （7）乙方出现将本合同项下全部或部分内容转包、将除甲方在采购文件明确允许以分包形式履行且乙方在投标环节已签订分包意向协议以外的服务内容分包的行为；

- （8）未经甲方书面同意，乙方将本合同项下属于甲方单方所有的成果作为己用或交付第三人使用的；
- （9）第三方指控并经有权机关认定甲方使用/接受乙方提供的产品/服务侵犯了该方的知识产权或其他权利，造成甲方损失的；

21.1.2. 乙方发出的终止

下述任一事件发生时，乙方有权立即发出终止意向通知：

- （1）甲方在本合同中的声明或保证在被证实是虚假的或未兑现，使乙方履行本合同的能力受到严重不利影响；
- （2）甲方无正当理由在逾期六个月（自应付日起算）后仍未履行支付义务。但因财政支付管理流程导致的支付延期除外。

21.1.3. 法律变更或政府行为

如果在本合同生效后，因法律变更及政府行为导致乙方部分或全部不能履行本合同项下主要义务，而这种变化和影响又不以甲方的意志为转移，甲乙双方应尽力就继续履行本合同进行协商，若不能达成一致，则一方可向另一方发出终止意向通知，双方仍协商不成的，本合同自终止意向通知到达对方之日起届满时终止。

21.1.4. 协商一致终止

在本合同履行期间，由各方协商一致可提前终止本合同。费用结算等问题由各方协商一致。

21.2. 双方协商

21.2.1. 终止意向通知发出之后，双方应在三十日内协商。

21.2.2. 如果双方就将要采取的措施达成一致意见，或者违约行为在指定期限内得到纠正，终止意向通知即自动失效。

21.3. 发出终止通知

如终止意向通知发出后，指定期限内违约方仍实施违约行为或违约行为仍未得到纠正，则另一方有权在指定期限届满后合同履约期满前任何时间发出终止本合同的书面通知，本合同自书面通知送达对方之日起终止。

21.4. 项目移交

无论因何种原因导致本合同终止，如需进行移交，在本合同终止之后，乙方都必须完成甲方合理要求的所有必要工作，将属于甲方的设备、数据和系统等资产移交给甲方。甲方可以选择由甲方或甲方指定的第三方接收。甲方设备、数据和系统的风险将在乙方向甲方（或其指定的第三方服务商）移交并经甲方书面确认之后转移到甲方。在风险转移到甲方之前，甲方的设备、数据和系统发生损坏、缺失、故障的，乙方应承担相应责任。

第八章 违约处理

22. 违约行为认定

除不可抗力情形外，签订本合同任一方不履行本合同的任一条款，均视为违约。

23. 违约责任承担方式

23.1. 继续履行

守约方有权暂时停止履行义务，并要求违约方继续履行本合同，待违约方纠正违约行为后恢复履行；守约方根据此款规定暂停履行义务不构成违约。

23.2. 赔偿

任何一方有权获得因另一方违约而使该方遭受的任何损失、支出和费用（包括但不限于评估费、鉴定费、律师费、诉讼费）的赔偿，该项赔偿由违约方支付。

23.3. 不减免和影响的事项

23.3.1. 违约方对违约责任的承担并不能减免其在本合同项下的其他任何义务。

23.3.2. 双方获得上述违约赔偿的权利不影响其在本合同项下的终止合同权利。

24. 违约责任

24.1. 甲方违约责任

24.1.1. 甲方未按照本合同约定，及时足额向乙方支付相应的合同金额，则乙方有权向甲方发出书面催告，如甲方在收到书面催告通知后的5日内仍未能支付的，则甲方除应支付应付未付的合同金额外，还应自收到书面催告通知后第1日按照应付未付金额 3 ‰的数额向乙方支付违约金。但因财政支付管理流程导致的支付延期除外。

24.1.2. 付款时间为甲方向财政部门提出支付申请的时间，而非款项实际到达乙方账户的时间。如因政府财政支付流程导致的支付延期，甲方不承担责任，也不能作为乙方延迟履行或不履行合同义务的抗辩理由。

24.1.3. 甲方无正当理由延迟组织验收或拒收乙方提供的、符合本合同约定的服务，每迟延一日，应按合同总额的3‰向乙方支付违约金。迟延累计超过 30 日（含 30 日），乙方有权终止合同，甲方仍应承担上述违约责任并向乙方支付已完成内容的全部款项。

24.1.4. 甲方支付的违约金和赔偿金总额不超过本合同金额的8 ‰。

24.2. 乙方违约责任

24.2.1. 服务交付延误

因乙方原因导致未能在本合同约定期限内交付产品或服务的，乙方应从逾期之日起每日按对应产品或服务总价的 3‰的数额向甲方支付违约金，逾期三十日以上的，甲方有权单方解除合同，乙方除应向甲方退还对应产品或服务的合同金额外，还应额外赔偿因此给甲方造成的直接经济损失（包括但不限于违约方的直接经济损失、预期可得利益损失以及为实现债权而支出的律师费、保全费、诉讼费、公证费、鉴定费、调查费等一切费用）。直接损失难以认定的，乙方应付违约金不应低于合同总金额的3 ‰。

24.2.2. 服务违约责任

乙方服务期限内须严格遵守服务质量承诺及相关管理规定确保服务质量，对于违反服务质量承诺和服务水平约定造成服务质量下降的，乙方应向甲方承担相应的违约责任。

24.2.3. 质量违约责任

24.2.3.1. 过程质量不合格

24.2.3.1.1 乙方需针对项目质量管理设置奖惩制度，对有关人员进行奖励或处罚。对在项目过程中发现质量问题及时上报、解决问题过程中表现优秀的人员给予表扬、奖励；对项目质量管理工作中失职、违章的个人，应予以处罚并提供相应的奖惩记录文件备查。

24.2.3.1.2 甲方应结合项目评价结果、项目验收效果等情况对乙方的质量管理情况进行考评，对质量管理工作不力、造成不良后果的，按甲方要求的合理期限内整改处理。

24.2.3.1.3 项目实施过程中，甲方聘请的监理单位有权在监理权限范围内向乙方发出整改通知单，乙方收到整改通知单，除按要求整改外，还应承担相应违约金，具体如下：乙方自收到第 2 份整改通知单起，乙方应承担的违约金为 0.1 万元/份；当收到的整改通知单数量达 5 份（含）以上时，乙方应承担的违约金为 0.2 万元/份。以上违约金经甲方确认后，甲方有权从合同尾款中直接扣除，若违约金累计超过尾款金额，则甲方有权就差额部分向乙方追索。（2 份以上，建议每份整改通知单，乙方承担违约金占合同总金额 0.5%，一般不超过 10 万；5 份以上，建议每份整改通知单，乙方承担违约金占合同总金额 1%，一般不超过 20 万左右；特别重大项目可另行商定）

24.2.3.2. 服务最终验收不合格

乙方交付的产品或服务不能满足甲方书面要求，甲方有权要求乙方整改，并由乙方承担由此产生的费用。乙方在甲方指定期限内拒绝整改或整改后仍不符合要求的，甲方有权解除合同，乙方除向甲方退还对应产品或服务的合同金额外，还应额外赔偿因此给甲方造成的直接经济损失（包括但不限于违约方的直接经济损失、预期可得利益损失以及为实现债权而支出的律师费、保全费、诉讼费、公证费、鉴定费、调查费等一切费用）。直接损失难以认定的，乙方应付违约金不应低于合同总金额的3 ‰。

24.2.4. 保密违约责任

乙方违反本合同保密条款的，应承担违约责任。如果给甲方造成经济损失，乙方应赔偿 甲方的直接经济损失及承担甲方因此而支出的一切合理费用（包括但不限于律师费、案件受理费、执行费、差旅费等）；如果因乙方恶意泄露信息资料，给甲方造成严重后果的，除应赔偿甲方的直接经济损失及承担甲方因此而支出的一切合理费用外， 甲方将通过法律手段追究乙方责任。

24.2.5. 转包、违规分包违约责任

24.2.5.1.乙方将本合同全部或肢解后转包的，一经发现， 甲方有权单方解除合同，并上报政府采购监管部门。甲方有权要求乙方按照对应转包的产品或服务合同金额予以赔偿外，若由此造成甲方其他直接损失的，乙方仍应予以赔偿。

24.2.5.2.除甲方在采购文件明确允许以分包形式履行，且乙方在投标环节已签订分包意向协议的情形外，将本合同项下服务内容进行分包的， 甲方有权要求乙方支付违约金，违约金应不低于合同总金额的 8%，而且甲方有权将违约金直接在剩余合同款项中予以扣减，并保留向政府采购监管部门进行投诉的权利。

24.2.6. 其他违约责任

24.2.6.1.乙方出现本合同第 21.1.1.条约定的情形之一，导致合同终止的，乙方应当按违约行为所对应金额的3%向甲方支付违约金，且赔偿甲方因此遭受的直接经济损失。

24.2.6.2.乙方支付的违约金和赔偿金总额不超过本合同金额的8%。

第九章 争议解决

25. 争议解决方式

25.1. 因履行合同所发生的一切争议，双方应友好协商解决，协商不成的，按下列第（2）种方式解决：

（1）提交中国广州仲裁委员会仲裁，仲裁裁决为终局裁决；

（2）双方均同意向甲方所在地人民法院提起诉讼，律师代理费用等均由败诉方承担。

25.2 在仲裁、诉讼进行过程中，双方将继续履行本合同未涉诉的其他部分（合同被解除或终止的除外）。

25.3 双方对于合同履行期间难以确定过错归属的，可以向双方认可的第三方机构申请鉴定，确认责任。鉴定费用由主张对方存在过错的一方先行垫付，最终由鉴定存在过错的一方承担。

第十章 保密范围及责任

26. 保密信息范围

26.1.在本合同执行过程中乙方接触的甲方所有业务信息（包括但不限于合同、计划、文档、方案、图纸、数据等）。

26.2.在本合同执行过程中接触的政府机关文件（包括但不限于内部发文、各类通知及会议记录等）。

26.3.其他详细保密条款内容见附件。

27. 保密责任

27.1. 乙方对其因身份、职务、职业或技术关系而知悉的甲方商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

27.2. 乙方不得以竞争为目的或出于私利或为第三人谋利而擅自保存、复制、披露、使用甲方商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露甲方的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露甲方的商业秘密和党政机关保密信息。由此造成甲方损失的，乙方应负责赔偿。

27.3. 乙方在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及 的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给本项目以外的其他方或乙方内部与本项目无关的任何人员。由此造成甲方损失的，乙方应负责赔偿。

27.4. 乙方对于工作期间知悉甲方的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。乙方应当在完成委托事项或本合同终止或解除时将资料原件全部返还甲方，并销毁所有复制件。

27.5.严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

27.6.未经甲方书面同意，乙方不得带领无关人员进入甲方办公场所，若从事政府项目工作，未经政府机关工作人员允许，不得进入与项目服务无关的政府机关其他办公场所。

27.7. 乙方的保密义务延及乙方聘用的员工、工作人员，如因其员工、工作人员导致本合同保密义务的违反或商业秘密的泄露， 由乙方承担全部违约责任。

27.8.涉及政府机关项目的保密内容可根据政府机关意见，相应增加修改，乙方予以接受并同意履行相应保密责任。

第十一章 项目资产权属

28. 项目资产权属

28.1.本合同不会引起任何已申请、登记的知识产权所有权的转移。

28.2.本项目所涉服务成果的知识产权包括___：

- (1) 软件著作权：（定制软件开发服务、定制软件升级服务、定制软件租赁服务一般都涉及）
- (2) 商标权；
- (3) 专利权；
- (4) 其他：无_____。

28.3. 甲乙双方一致同意，本合同所涉成品软件租赁服务成果的知识产权归属按下列第（3）种方式处理；本合同所涉 基础设施租赁和运维服务成果的知识产权归属按下列第（4）种方式处理。

（1）乙方负责开发软件服务，包括代码编写、调试、测试等开发工作，乙方为履行本合同义务所形成的服务成果的知识产权归甲方单独所有。

（2）乙方负责提供定制软件租赁服务， 甲方基于本合同约定委托乙方定制开发的产品、程序、服务等知识产权归甲、乙方共同所有，乙方应按甲方书面要求交付该共有部分的源代码；乙方在共有部分的基础上进行二次开发的及对二次开发形成的产品、程序等财产进行处置的，需经甲方书面同意，二次开发所形成的产品、程序、服务等知识产权归开发者所有，共有部分仍归甲、乙方共同所有。乙方根据甲方授权，利用项目成果申请的商标、专利或输出的图片、视频等受知识产权保护的成果物， 甲方有权无条件永久使用。

（3）乙方负责提供运营服务或成品软件租赁服务， 乙方为履行本合同义务所形成的所有服务成果的知识产权（除成品软件开发涉及的知识产权）归甲方单独所有。

（4）本项目仅包含基础设施服务租用或运维服务，不涉及知识产权权属转移。

28.4.本合同所涉及的数据所有权归政府所有。数据资产的管理应遵循财政部《关于加强数据资产管理的指导意见》（财资〔2023〕141号）及其他相关法律、法规、政策要求。

28.5.本项目所涉服务成果的知识产权由甲方单独所有的，甲方在保持知识产权归属不变的前提下，授权乙方在依托“粤复用 ”进行复用推广的范围内使用以下权利：

（1）软件著作发表权的使用，乙方有权将基于本项目服务成果提炼形成的产品、组件上架“粤复用 ”，上架产品、组件的软件著作权归属与本项目服务成果保持不变，乙方应在“粤复用 ”上明确说明甲方单独享有上架产品、组件的软件著作权。

（2）软件著作权修改权与复制权的使用，乙方依托“粤复用 ”复用推广本项目服务成果或提炼形成的上架产品、组件时，可按照复用需求复制和修改本项目服务成果，形成复用案例并上架“粤复用 ”，并向甲方报备复用案例。

（3）除第（1）、（2）款授予的权利外，乙方依托“粤复用 ”进行复用推广涉及软件著作署名权、发行权、出租权、信息网络传播权、翻译权以及甲方享有的其他权利的使用，须事先经甲方书面同意或与甲方另行签署书面补充协议确定。

（4）乙方须事先经甲方书面同意或与甲方另行签署书面补充协议的情况下，才能在“粤 复用 ”范围以外以任何形式使用本项目服务成果或上架产品、组件的相关全部或部分知识产权权利。

28.6.本项目所涉服务成果中，对于知识产权由甲、乙双方共同所有的部分，在保持知识产权归属不变的前提下，双方约定在依托“粤复用 ”进行复用推广的范围内按以下方式行使权利：

（1）软件著作发表权的使用， 甲方将本项目服务成果形成应用案例，乙方提炼形成产品、组件，乙方应在上架“粤复用 ”时明确说明甲、乙双方共同所有软件著作权的情况。

（2）软件著作修改权与复制权的使用， 甲、乙双方依托“粤复用 ”复用推广本项目服务 成果时，乙方可按照复用需求复制和修改本项目服务成果，形成复用案例并上架“粤复用 ”，并向甲方报备复用案例。

（3）除第（1）、（2）款授予的权利外，乙方依托“粤复用 ”进行复用推广涉及软件著作署名权、发行权、出租权、信息网络传播权、翻译

权以及其他权利的使用，任何一方使用时应事先书面通报对方并对外明确软件著作权共同所有的情况。未经甲方同意，乙方不得转让、质押、赠予等任何方式处置其享有的软件著作权或其组成部分的著作权或相应权益；否则，为无效行为且严重侵权，须赔偿甲方全部损失。

(4) 乙方在“粤复用”范围以外使用双方共同所有知识产权的，应由甲方双方书面协商一致后行使，乙方应当保证合法合规使用双方共同所有知识产权，否则造成甲方损失的，乙方还应承担全部赔偿责任。

(5) 乙方申报商标时应经甲方同意，明确甲方有权无条件永久使用商标权。

28.7. 乙方提供的相关软件应是自行开发的产品或具备合法、合规授权，满足知识产权、安全等保三级等方面的有关规定和要求。

28.8. 乙方保证向甲方提供的服务成果不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因乙方提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

第十二章其他约定

29. 其他约定

29.1. 合同构成

29.1.1. 下列文件均为本合同不可分割的组成部分，具有同等法律效力：

- (1) 中标通知书；
- (2) 采购文件；
- (3) 乙方中标的投标文件；
- (4) 在合同实施过程中双方共同签署的补充协议（若有）；
- (5) 分包意向协议（若有）；
- (6) 变更文件（若有）；
- (7) 合同附件。

上述文件先后解释顺序为：在合同实施过程中双方共同签署的补充协议、变更文件、本合同书、合同附件、分包意向协议、中标通知书、采购文件、乙方中标的投标文件。补充协议之间如有冲突，以对乙方要求较高或对甲方更有利的条款为准。

29.2. 合同变更与修订

29.2.1. 除另有约定，本合同任何修改、补充或变更必须经双方协商一致，并书面签订补充协议。

29.2.2. 如果本合同的任何条款不合法、无效或不能执行，则：

- (1) 并不影响其他条款的效力和执行；
- (2) 双方应商定对不合法、无效或不能执行的条款进行修改，使之合法、有效并可执行；修改或更改应尽可能平衡双方之间的利益。

29.2.3. 项目变更时为确保效率，如无涉及项目合同金额变动且甲方认为没有必要的，可按照甲乙双方书面确认的往来文件立即实施。如涉及项目合同金额变动或甲方认为确有必要的，乙方需按甲方要求完成变更申请审批工作，并双方必须就相关变更事项签订补充协议。

29.3. 合同适用法律

本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决适用中华人民共和国法律。

29.4. 不弃权

除非另有规定，一方未行使或迟延履行使本合同项下的权利、权力并不构成放弃这些权利、权力，而单一或部分行使这些权利、权力并不排斥行使任何其他权利、权力。

29.5. 通知

29.5.1. 本合同约定的联系地址、联系方式为甲乙双方唯一联系地址、联系方式。甲、乙双方因履行本合同而需由一方发给对方的任何通知应以书面方式发出。该通知可以专人送达、传真、电子邮件、特快专递或挂号方式送达的方式发出。所有的通知应送达本合同项下对方当事人的地址或该方事先通知的其他地址或传真号码。该联系地址或联系方式有变动的，应至少提前三日书面通知对方。双方发生争议后，甚至进入诉讼程序，该联系地址、联系方式仍为有效。

29.5.2. 上述通知、要求或信息，以专人送达的，以受送达人在送达回执上的签收时间为送达日期；以传真方式送达的，以发送之日为送达日期；以电子邮件方式送达的，以到达受送达人特定系统的日期为送达日期；以特快专递或挂号方式送达的，以受送达人在相应邮寄凭证上签收之日为送达日期。上述联系地址或联系方式发生变动且未及时书面通知另一方的，另一方按原地址邮寄相关材料即视为已履行送达义务。

29.6. 合同生效条件

本合同经甲乙双方法定代表人或授权委托代理人签字，并盖章后生效。

29.7. 合同份数

本合同一式伍份， 甲方执贰份，乙方执叁份（含采购代理机构备案壹份），具有同等法律效力。

29.8. 合同页数

本合同正文（不含封面、编写说明及签署页）合计 页 **A4** 纸张，附件__份共__页 **A4** 纸张。缺页之合同为无效合同。

附件：

- 1.详细服务内容及技术要求
- 2.验收要求
- 3.乙方团队人员清单
- 4.服务价格明细（若有）
- 5.保密承诺书
- 6.反商业贿赂协议
- 7.软件委托开发协议书（若有）
- 8.服务违约行为表（若有）

（以下无合同正文）

(签署页)

委托方(甲方): 广东省国土资源技术中心

(盖章)

住 所 地: 广东省广州市海珠区国土资源数字化综合楼

法定代表人/委托代理人: (签名/章)

项目联系人:

联系方式:

通讯地址: 广东省广州市海珠区国土资源数字化综合楼

电 话:

传 真:

电子信箱:

年 月 日

受托方(乙方): (盖章)

住 所 地:

法定代表人/委托代理人: (签名/章)

项目联系人:

联系方式:

通讯地址:

电 话:

传 真:

电子信箱:

年 月 日

附件 1.详细服务内容及技术要求

附件 2.验收要求

参照我省政务信息化项目验收相关规范开展验收工作。按照《广东省政务服务数据管理局政务信息化项目验收管理工作指引》开展验收工作（若有更新则以验收时最新印发版本为准）。

1.验收标准和条件

- （1）符合本项目采购文件中采购需求描述相关技术要求和乙方投标文件中承诺的相应技术指标或标准。
- （2）甲方与乙方在项目实施过程中约定的其他相关技术要求。

2.验收方式

由甲方组织专家进行验收，必要时，可邀请第三方机构进行验收。

附件 3. 乙方团队人员清单

提出乙方拟投入的团队人员名单，及各角色职责与分工。

姓名	性别	年龄	学历	职称	同类工 作年限	公司 职务	本项目角色	承担工作
项目主要人员简历（毕业院校、曾任职、专长、承担同类项目历史情况）								

附件 4.服务价格明细（若有）

提出乙方服务价格构成及分项明细表。

保密承诺书

致：

为保护合作方甲方的合法利益，保证合作双方实现顺利合作，避免因信息泄露而给甲方造成损失，本项目的服务方_____以及参与本项目的
的所有员工承诺遵守本保密承诺书内容。

一、保密信息定义

本承诺书所称的“保密信息”是指所有涉密信息、商业秘密、技术秘密、通信或与该项目相关的其他信息，无论是书面的、口头的、图形的、电磁的或其他任何形式的信息，包括（但不限于）数据、用户名、口令、产品、文件、规划、方案、技术、方法、仪器设备和
其他信息及文档等，上述信息在本项目以如下形式确定：

- 1. 甲方在项目实施中为乙方及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；
- 2.在对甲方提供服务工作中涉及的业务及技术文档，包括政策、方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档，测试和测试产生的数据等；
- 3.服务过程中产生的所有成果为保密的内容；
- 4.其他甲方合理认为并申明属于保密信息的内容。

二、保密要求

我公司在国家相关法律法规、规章政策所规定的前提下，全力限制“保密信息”的使用范围以利保密防范，并仅用于为甲方提供服务。在未经甲方书面
形式授权下，我公司不会直接或间接使用“项目资料”的利益或目的性的任何专有信息，亦不会把任何专用信息披露给他人,我公司的所有员工均有义务受约束，并负有保密的义务。

- 1.承诺人始终对保密资料保密，不在项目之外使用甲方提供的保密信息及因履行本项目而掌握的保密信息。
- 2.未经甲方书面同意，不向任何第三方提供保密信息以及可以接触上述保密信息的手段，包括在公开场合展览，公开对外宣传，作为文章、讯息、参考数据发表等。
- 3. 只向项目相关人员（包括各自的领导、同事和雇员等）为商讨合作项目而有需要知悉保密信息的人士披露保密信息；并保证上述各相关人员的
行为将会符合本守则的规定。
- 4.在商讨合作项目的过程中，若需向第三方披露甲方的保密信息，应取得甲方书面许可，并要求该第三方不得向任何其他人士泄露保密信息。
- 5.有关保密的内容和义务，未经甲方解封则长期有效。

承诺人：

（法定代表人或委托代理人签字并盖单位公章）

日期：

反商业贿赂协议

根据《关于开展治理商业贿赂专项工作的意见》（中办发〔2006〕9号）以及有关项目服务、廉政建设的规定，为做好项目服务中的反商业贿赂工作，建立起责任机制、督查机制和保障机制，保证项目服务高效优质，保证建设资金的安全和有效使用以及投资效益，本项目

甲方与乙方特订立如下协议。

一、 甲乙双方的权利和义务

- 1.严格遵守党的政策规定和国家有关法律法规及广东省委、省政府关于反商业贿赂和加强党风廉政建设的有关规定。
- 2.严格执行本项目的合同文件， 自觉按合同办事。
- 3.双方的业务活动坚持公开、公正、诚信、透明的原则(法律认定的商业秘密和合同文件另有规定除外)，不得损害国家和集体利益，违反项目管理规章制度。
- 4.建立健全反商业贿赂和廉政制度，开展相关教育，设立反商业贿赂和廉政告示牌。公布举报电话，监督并认真查处违法违纪行为。
- 5.发现对方在业务活动中有违反商业贿赂和廉政规定的行为，有及时提醒对方纠正的权利和义务。
- 6.发现对方严重违反合同义务条款的行为，有向其上级有关部门举报、建议给予处理并要求告知处理结果的权利。
- 7.双方或双方与系统设计、软件开发、系统集成、设备材料供应等相关单位不得串通、弄虚作假谋取不正当利益或降低服务质量等损害国家利益。
- 8.乙方遵守《反商业贿赂协议》情况纳入甲方对乙方的绩效考评范围。

二、 甲方的义务

- 1.甲方及其工作人员不索要或接受乙方的礼金、有价证券和贵重物品，不得在乙方报销任何应由甲方或甲方工作人员个人支付的费用等。
- 2.甲方工作人员不得参加乙方安排的超标准宴请和娱乐活动；不得接受乙方提供的通讯工具、交通工具和高档办公用品等。
- 3.甲方及其工作人员不得要求或者接受乙方为其住房装修、婚丧嫁娶活动、配偶子女的工作安排以及出国出境、旅游等提供方便等。
- 4.甲方工作人员及其配偶、子女不得从事与项目有关的材料设备供应、服务承包、劳务活动等。
- 5.甲方及其工作人员不得利用职权插手项目活动谋求不正当利益，不得以任何理由向乙方推荐项目建设相关单位或推销材料，不得要求乙方购买合同规定外的材料和设备。
- 6.甲方工作人员要秉公办事，不准营私舞弊，不准利用职权从事各种个人有偿中介活动和安排介绍服务团队。

三、乙方义务

- 1.乙方不得以任何理由向甲方及其工作人员、服务单位行贿或馈赠礼金、有价证券、贵重礼品。
- 2.乙方不得以任何名义为甲方及其工作人员报销应由甲方单位或个人支付的任何费用。
- 3.乙方不得以任何理由安排甲方工作人员参加超标准宴请及娱乐活动。
- 4.乙方不得为甲方单位和个人购置或提供通讯工具、交通工具和高档办公用品等。

四、违约责任

- 1.甲方及其工作人员违反本合同第一、二条，按管理权限，依据有关规定给予党纪、政纪或组织处理；涉嫌犯罪的，移交司法机关追究刑事责任；给乙方单位造成经济损失的，应予以赔偿。
- 2.乙方及其工作人员违反本合同第一、三条，按合同金额的 50%向甲方支付违约金，同时按管理权限，依据有关规定给予党纪、政纪组织处理；给甲方单位造成经济损失的，应予以经济赔偿。

五、双方约定，双方有义务对合同执行情况开展自查自纠，并自觉接受有关部门监督。

六、本协议有效期为甲乙双方签署之日起至该项目服务期满止。

七、本协议作为_____合同的附件，与上述合同具有同等的法律效力，经合同双方签署后生效。

委托方（甲方）： （盖单位公章） 受托方（乙方）： （盖公章）
法定代表人 法定代表人

或其委托代理人（签名/章）： 或其委托代理人（签名/章）：

日期： 日期：

软件委托开发协议书

委托方：

受托方：

鉴于，本协议受托方为计算机软件专业开发机构，能够进行创造性的软件开发活动。并且，本协议委托方有意委托受托方完成 XXX 系统（版本号 VX.X）软件的开发工作。为了规范各方的权利义务，在《中华人民共和国著作权法》和《中华人民共和国民法典》等相关法规之规定，订立本协议书，各方共同遵守：

第一条、项目宗旨

为完成XXX 系统（版本号 VX.X）软件（“本软件”）的开发工作，并由本协议约定主体享有开发成果而拟定本软件委托开发协议书。

第二条 委托项目和范围

受托方负责开发本软件，包括本软件的代码编写、调试、测试等开发工作。

第三条 委托期限

委托期限为自本协议签署之日起至本项目最终验收之日止。

第四条 委托方式

- 1. 受托方应严格依照双方约定开发目标完成本软件开发工作，不得随意更改本软件的重大能和事项。
- 2. 委托方应就本软件开发工作予以受托方相应的支持。

第五条 知识产权

- 1. 软件著作权的全部权利归双方共同所有/委托方所有。
- 2. 受托方在编写软件的过程中，不得有侵犯他人知识产权的行为，否则，应单独对外承担全部侵权责任。

第六条 协议变更及转让

- 1. 经合作各方协商同意，本协议可以作相应变更；
- 2. 本协议任何一方未经与其他各方协商，擅自变更本协议条款或者将本协议权利义务转让他人，均为无效。

第七条 协议终止

本协议因以下事由之一得终止：

- ①经本协议各方协商一致；②委托开发项目因技术原因，根本不能完成；③委托开发项目违反法律被撤销。

第八条 纠纷的解决

本协议各方之间如发生纠纷，应共同协商，本着有利于事业发展的原则予以解决。如协商不成，可以诉诸法院。

第九条 本协议自各方签字（或盖章）之日起生效，

委托方（签章）

受托方（签章）

签署时间： 年 月 日

服务违约行为表

一、重大违约行为

乙方服务期限内的违约行为造成云平台整体故障（非不可抗力条件下）或重大安全事故的（根据其严重程度分为 A 级事件和 B 级事件）。
违约金=当月所有业务系统云服务月租费（云服务月租费按省财政厅最新批复的标准执行）

表：重大违约行为表

类别	范围	影响	影响时间	事件级别	次数
----	----	----	------	------	----

二、严重违约行为

乙方在服务期内的违约行为对用户业务系统产生一定的经济损失，但其影响和经济损失未达到重大违约行为中规定的 B 级事件的。
违约金=对应业务系统云合同金额/服务月数*违约金系数（违约金系数参见《严重违约行为表》）

表：严重违约行为表

序号	问题描述	违约金系数
----	------	-------

三、一般违约行为

乙方在服务期的违约行为对用户业务系统造成的影响未达到重大违约行为和严重违约行为的其他违约行为。
违约金=对应业务系统云合同金额/服务月数*违约金系数（违约金系数参见《一般违约行为表》）

表：一般违约行为表

序号	问题描述	违约金系数
----	------	-------

第六章 投标文件格式与要求

投标人应提交证明其有资格参加投标和中标后有能力履行合同的相关文件，并作为其投标文件的一部分，所有文件必须真实可靠、不得伪造，否则将按相关规定予以处罚。

1.法人或者其他组织的营业执照等证明文件，自然人的身份证明：

法人包括企业法人、机关法人、事业单位法人和社会团体法人；其他组织主要包括合伙企业、非企业专业服务机构、个体工商户、农村承包经营户；自然人是指《中华人民共和国民法典》（以下简称《民法典》）规定的具有完全民事行为能力、能够承担民事责任和义务的公民。如投标人是企业（包括合伙企业），要提供在工商部门注册的有效“企业法人营业执照”或“营业执照”；如投标人是事业单位，要提供有效的“事业单位法人证书”；投标人是非企业专业服务机构的，如律师事务所，会计师事务所要提供执业许可证等证明文件；如投标人是个体工商户，要提供有效的“个体工商户营业执照”；如投标人是自然人，要提供有效的自然人身份证明。

这里所指“其他组织”不包括法人的分支机构，由于法人分支机构不能独立承担民事责任，不能以分支机构的身份参加政府采购，只能以法人身份参加。“但由于银行、保险、石油石化、电力、电信等行业具有其特殊性，如果能够提供其法人给予的相应授权证明材料，可以参加政府采购活动”。

2.财务状况报告，依法缴纳税收和社会保障资金的相关材料（详见资格性审查表要求）

3.具有履行合同所必需的设备和专业技术能力的声明。

4.投标人参加政府采购前三年内在经营活动中没有重大违法记录书面声明函。

5.信用记录查询

（1）查询渠道：通过“信用中国”网站(www.creditchina.gov.cn)和“中国政府采购网”（www.ccgp.gov.cn）进行查询；

（2）查询截止时点：提交投标文件截止日当天；

（3）查询记录：对列入失信被执行人、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、信用报告进行查询；

采购人或采购代理机构应当按照查询渠道、查询时间节点、查询记录内容查询，并存档。对信用记录查询结果中显示投标人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的投标人作无效投标处理。

6. 按照招标文件要求，投标人应当提交的资格、资信证明文件。

投标文件封面

（项目名称）

投标文件封面

（正本 / 副本）

采购计划编号：**440001-2026-17063**

采购项目编号：**ZZ0260087**

所投采购包：第 包

（投标人名称）

年 月 日

投标文件目录

- 一、投标函
- 二、开标一览表
- 三、分项报价表
- 四、政策适用性说明
- 五、关于符合本国产品标准的声明函等有关证明文件
- 六、法定代表人证明书
- 七、法定代表人授权书
- 八、投标保证金
- 九、提供具有独立承担民事责任的能力的证明材料
- 十、资格性审查要求的其他资质证明文件
- 十一、承诺函
- 十二、中小企业声明函
- 十三、监狱企业
- 十四、残疾人福利性单位声明函
- 十五、联合体共同投标协议书
- 十六、投标人业绩情况表
- 十七、技术和服务要求响应表
- 十八、商务条件响应表
- 十九、履约进度计划表
- 二十、各类证明材料
- 二十一、采购代理服务费支付承诺书
- 二十二、需要采购人提供的附加条件
- 二十三、询问函、质疑函、投诉书格式
- 二十四、项目实施方案、质量保证及售后服务承诺等
- 二十五、政府采购投标（响应）担保函
- 二十六、政府采购履约担保函、采购合同履行保险凭证

格式一：

投标函

致：广东志正招标有限公司

你方组织的“广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）”项目的招标[采购项目编号为：ZZ0260087]，我方愿参与投标。

(投标人名称)作为投标人正式授权(授权代表全名,职务)代表我方全权处理有关本投标的一切事宜。

我方确认收到贵方提供的“广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）”项目的招标文件的全部内容。

我方已完全明白招标文件的所有条款要求，并申明如下：

（一）按招标文件提供全部标的投标总价详见《开标一览表》。

（二）本投标文件的有效期为从提交投标（响应）文件的截止之日起**90**日历天。在此提交的资格证明文件均至投标截止日有效，如有在投标有效期内失效的，我方承诺在中标后补齐一切手续，保证所有资格证明文件直至采购合同终止日有效。

（三）我方明白并同意，在规定的开标日之后，投标有效期之内撤销投标或中标后不按规定与采购人签订合同或不提交履约保证金，则贵方将不予退还投标保证金。

（四）我方愿意向贵方提供任何与本项报价有关的数据、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。

（五）我方理解贵方不一定接受最低投标价或任何贵方可能收到的投标。

（六）我方如果中标，将保证履行招标（采购）文件及其澄清、修改文件（如果有）以及投标（响应）文件中的全部责任和义务，按质、按量、按期完成《合同书》中的全部任务。

（七）我方作为法律、财务和运作上独立于采购人、采购代理机构的投标人，在此保证所提交的所有文件和全部说明是真实的和正确的。

（八）我方投标报价已包含应向知识产权所有权人支付的所有相关税费，并保证采购人在中国使用我方提供的标的时，如有第三方提出侵犯其知识产权主张的，责任由我方承担。

（九）我方接受采购人委托向贵方支付代理服务费，项目总报价已包含代理服务费，如果被确定为中标人，承诺向贵方足额支付。（若采购人支付代理服务费，则此条不适用）

（十）我方与其他投标人不存在单位负责人为同一人或者存在直接控股、管理关系。

（十一）投标人未存在《政府采购法实施条例》第十八条第二款规定的情形：

（1）对于除整体设计、规范编制或者项目管理、监理、检测等服务以外的采购项目:即未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务；

（2）对于整体设计、规范编制或者项目管理、监理、检测等服务的项目:即未成为本项目除前期整体设计、规范编制或者项目管理、监理、检测等服务以外的其它采购活动中标商(或成交商)；

（3）对于设计施工一体化的项目:即未为本项目提供规范编制或者项目管理、监理、检测等服务。

（十二）我方承诺遵守《中华人民共和国民法典》有关规定和《中华人民共和国妇女权益保障法》中关于“劳动和社会保障权益”的有关要求。

（十三）我方具备《中华人民共和国政府采购法》第二十二条规定的条件，声明如下：

（1）我方参加本项目政府采购活动前**3**年内在经营活动中没有以下违法记录：因违法经营被禁止参加政府采购活动的期限已届满；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。

（2）我方符合法律、行政法规规定的其他条件。

（十四）如我方中标，将保证投标文件所提供的材料（包括需要年审、继续教育等完成后才能执业的行政许可、人员证书等情形），如果有效期未能覆盖项目（包组）合同履行期的，将提前按规定办理延期手续，确保合同顺利履行。

（十五）我方对在本函及投标文件中所作的所有承诺承担法律责任。

(十六) 以上内容如有虚假或与事实不符的, 评标委员会可将我方做无效投标处理, 我方愿意承担相应的法律责任。

(十七) 所有与本招标有关的函件请发往下列地址:

地 址: _____ 邮政编码: _____

电 话: _____

传 真: _____ 电子邮箱: _____

代表姓名: _____ 职 务: _____

投标人法定代表人 (或法定代表人授权代表) 签字或盖章: _____

投标人名称 (盖章): _____

日期: 年 月 日

格式二：

开标一览表

注：投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成开标一览表，若在投标文件中出现非系统生成的开标一览表，且与投标客户端生成的开标一览表信息内容不一致，以投标客户端在线填写报价并生成的内容为准。（下列表样仅供参考）

采购项目编号：

项目名称：

投标人名称：

序号	采购项目名称/采购包名称	投标报价（元/%）	交货或服务期	交货或服务地点
1				

投标人签章：_____

日期： 年 月 日

格式三：

分项报价表

注：投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成分项报价表，若在投标文件中出现非系统生成的分项报价表，且与投标客户端生成的分项报价表信息内容不一致，以投标客户端在线填写报价并生成的内容为准。（下列表样仅供参考）

采购项目编号：

项目名称：

投标人名称：

采购包：

货币及单位：人民币/元

品目号	序号	货物名称	规格型号	品牌	产地	制造商名称	单价	数量	总价
1									

品目号	序号	服务名称	服务范围	服务要求	服务时间	服务标准	单价	数量	总价
1									

投标人签章：_____

日期： 年 月 日

格式四：

政策适用性说明

按照政府采购有关政策的要求，在本次的技术方案中，采用符合政策的小型或微型企业产品、节能产品、环境标志产品，主要产品与核心技术介绍说明如下：

序号	主要产品/技术名称（规格型号、注册商标）	制造商(开发商)	制造商企业类型	节能产品	环境标志产品	认证证书编号	该产品报价在总报价中占比（%）
1							
2							
3							
4							
5							
...							

注：1.制造商为小型或微型企业时才需要填“制造商企业类型”栏,填写内容为“小型”或“微型”；

2.“节能产品、环境标志产品”须填写认证证书编号，并在对应“节能产品”、“环境标志产品”栏中勾选，同时提供有效期内的证书复印件（加盖投标人公章）

投标人名称（盖章）：_____

日期： 年 月 日

格式五：关于符合本国产品标准的声明函等有关证明文件（如适用）

注：

1. 供应商提供本国产品应符合《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号），在投标文件中出具《关于符合本国产品标准的声明函》或财政部会同有关部门规定的有关证明文件；当采购项目或者采购包中含有多种产品的，供应商还应当提供《关于本国产品比例的承诺函》（见下附件3，格式内容仅供参考）
2. 供应商提供虚假《声明函》、虚假证明文件谋取中标、成交的，依照政府采购法律法规规定追究相应责任。

附件1

中国境内生产的组件成本核算基本规则

产品在中国境内生产的组件成本，一般按照其二级组件的相关成本进行核算。按照产品的一级组件进行成本核算能够满足中国境内生产的组件成本判定需求的，可以按照一级组件的相关成本进行核算。

1. 产品的一级组件是指直接组成产品的组件。产品的二级组件是指直接组成产品一级组件的组件。一级组件不可分解的，视同二级组件。
2. 二级组件在中国境内生产的，其全部成本计入中国境内生产的组件成本；二级组件不在中国境内生产的，其成本不计入中国境内生产的组件成本。
3. 产品总成本和组件成本以相关会计核算数据、采购合同、进货记录等为基础进行计算。
4. 需要对成本核算规则予以进一步明确的其他有关事项，由财政部会同有关部门另行规定。

附件2

关于符合本国产品标准的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）的规定，本公司（单位）提供的以下产品属于本国产品。具体情况如下：

1. （产品名称1），生产厂为（厂名），厂址为（生产厂址）。（产品名称1）的中国境内生产的组件成本占比 $\geq$ （规定比例）。（产品名称1）的（关键组件）在中国境内生产。（产品名称1）的（关键工序）在中国境内完成。
2. （产品名称2），生产厂为（厂名），厂址为（生产厂址）。（产品名称2）的中国境内生产的组件成本占比 $\geq$ （规定比例）。（产品名称2）的（关键组件）在中国境内生产。（产品名称2）的（关键工序）在中国境内完成。
3.

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）： _____

日期： _____ 年 _____ 月 _____ 日

注：

1. 产品如有型号，请在“产品名称”栏一并填写。
2. 生产厂名与厂址应与生产厂营业执照载明的相关信息保持一致。
3. 该产品的中国境内生产的组件成本占比相关要求实施前，“规定比例”栏可不填，下同。
4. 该产品的关键组件要求实施前，“关键组件”栏可不填，下同。
5. 该产品的关键工序要求实施前，“关键工序”栏可不填，下同。

附件3（当采购项目或者采购包中含有多种产品的，供应商还应当提供本承诺函，格式内容仅供参考）

关于本国产品比例的承诺函（如适用）

本公司（单位）郑重承诺，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）的规定，本公司（单位）提供的符合本国产品标准的产品成本之和占提供的全部产品成本之和的比例达到80%以上。

本公司（单位）对上述承诺内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：_____

日期：_____年_____月_____日

附件4

本国产品标准有关证明材料（如适用）

1. 供应商认为需提供其他资料。
2. 财政部会同有关部门规定的有关证明文件。

格式六：

（投标人可使用下述格式，也可使用广东省工商行政管理局统一印制的法定代表人证明书格式）

法定代表人证明书

_____现任我单位_____职务，为法定代表人，特此证明。

有效期限：_____

附：代表人性别：_____年龄：_____身份证号码：_____

注册号码：_____企业类型：_____

经营范围：_____

投标人名称（盖章）：_____

地址：_____

法定代表人（签字或盖章）：_____

职务：_____

日期： 年 月 日

格式七:

法定代表人授权书格式

(对于银行、保险、电信、邮政、铁路等行业以及获得总公司投标授权的分公司，可以提供投标分支机构负责人授权书)

法定代表人授权书

致: 广东志正招标有限公司

本授权书声明: _____是注册于 (国家或地区) 的 (投标人名称) 的法定代表人, 现任_____职务, 有效证件号码: _____。现授权 (姓名、职务) 作为我公司的全权代理人, 就“广东省国土资源技术中心政务信息化运维(2026年)项目(基础设施及运行维护服务)”项目采购[采购项目编号为ZZ0260087]的投标和合同执行, 以我方的名义处理一切与之有关的事宜。

本授权书于_____年_____月_____日签字生效, 特此声明。

投标人(盖章): _____

地址: _____

法定代表人(签字或盖章): _____

职务: _____

被授权人(签字或盖章): _____

职务: _____

日期: 年 月 日

格式八：

投标保证金

采购文件要求递交投标保证金的，投标人应在此提供保证金的凭证的复印件。

格式九：

提供具有独立承担民事责任的能力的证明材料

格式十：

资格审查要求的其他资质证明文件

具有履行合同所必需的设备和专业技术能力

格式十一：

（对于采购需求写明“提供承诺”的条款，供应商可参照以下格式提供承诺）

承诺函

致：广东省国土资源技术中心（广东省基础地理信息中心）

对于_____项目（项目编号：_____），我方郑重承诺如下：

如中标/成交，我方承诺严格落实采购文件以下条款：(建议逐条复制采购文件相关条款原文)

（一）星号条款

- 1.
- 2.
- 3.

.....

（二）三角号条款

- 1.
- 2.
- 3.

.....

（三）非星号、非三角号条款

- 1.
- 2.
- 3.

.....

特此承诺。

供应商名称（盖章）：_____

日期： 年 月 日

格式十二：

（以下格式文件由供应商根据需要选用）

中小企业声明函（所投产品制造商为中小企业时提交本函，所属行业应符合采购文件中明确的本项目所属行业）

中小企业声明函（货物）

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（单位名称）的（项目名称）采购活动，提供的货物全部由符合政策要求的中小企业制造。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）行业；制造商为（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）；
2. （标的名称），属于（采购文件中明确的所属行业）行业；制造商为（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： 年 月 日

- 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
- 2：投标人应当对其出具的《中小企业声明函》真实性负责，投标人出具的《中小企业声明函》内容不实的，属于提供虚假材料谋取中标。在实际操作中，投标人希望获得中小企业扶持政策支持的，应从制造商处获得充分、准确的信息。对相关制造商信息了解不充分，或者不能确定相关信息真实、准确的，不建议出具《中小企业声明函》。

中小企业声明函（承建本项目工程为中小企业或者承接本项目服务为中小企业时提交本函，所属行业应符合采购文件中明确的本项目所属行业）

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（单位名称）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）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）；

2. （标的名称），属于（采购文件中明确的所属行业）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： 年 月 日

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。

2：投标人应当自行核实是否属于小微企业，并认真填写声明函，若有虚假将追究其责任。

格式十三：

（以下格式文件由供应商根据需要选用）

监狱企业

提供由监狱管理局、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。

格式十四：

（以下格式文件由供应商根据需要选用）

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_____单位的_____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： 年 月 日

注：本函未填写或未勾选视作未做声明。

格式十五：

（以下格式文件由供应商根据需要选用）

联合体共同投标协议书

立约方：（甲公司全称）

（乙公司全称）

（.....公司全称）

（甲公司全称）、（乙公司全称）、（.....公司全称）自愿组成联合体，以一个投标人的身份共同参加（采购项目名称）（采购项目编号）的响应活动。经各方充分协商一致，就项目的响应和合同实施阶段的有关事务协商一致订立协议如下：

一、联合体各方关系

（甲公司全称）、（乙公司全称）、（.....公司全称）共同组成一个联合体，以一个投标人的身份共同参加本项目的响应。（甲公司全称）、（乙公司全称）、（.....公司全称）作为联合体成员，若中标，联合体各方共同与（采购人）签订政府采购合同。

二、联合体内部有关事项约定如下：

1.（甲公司全称）作为联合体的牵头单位，代表联合体双方负责投标和合同实施阶段的主办、协调工作。

2.联合体将严格按照文件的各项要求，递交投标文件，切实执行一切合同文件，共同承担合同规定的一切义务和责任，同时按照内部职责的划分，承担自身所负的责任和风险，在法律上承担连带责任。

3.如果本联合体中标，（甲公司全称）负责本项目_____部分，（乙公司全称）负责本项目_____部分。

4.如中标，联合体各方共同与（采购人）签订合同书，并就中标项目向采购人负责有连带的和各自的法律责任；

5.联合体成员（公司全称）为（请填写：小型、微型）企业，将承担合同总金额_____%的工作内容（联合体成员中有小型、微型企业时适用）。

三、联合体各方不得再以自己名义参与本采购包响应，联合体各方不能作为其它联合体或单独响应单位的项目组成员参加本采购包响应。因发生上述问题导致联合体响应成为无效报价，联合体的其他成员可追究其违约责任和经济损失。

四、联合体如因违约过失责任而导致采购人经济损失或被索赔时，本联合体任何一方均同意无条件优先清偿采购人的一切债务和经济赔偿。

五、本协议在自签署之日起生效，有效期内有效，如获中标资格，合同有效期延续至合同履行完毕之日。

六、本协议书正本一式_____份，随投标文件装订_____份，送采购人_____份，联合体成员各一份；副本一式_____份，联合体成员各执_____份。

甲公司全称：____（盖章）____，乙公司全称：____（盖章）____，.....公司全称：____（盖章）____，
____年____月____日，____年____月____日，____年____月____日

注：1. 联合响应时需签本协议，联合体各方成员应在本协议上共同盖章确认。

2. 本协议内容不得擅自修改。此协议将作为签订合同的附件之一。

格式十六：

（以下格式文件由供应商根据需要选用）

投标人业绩情况表

序号	客户名称	项目名称及合同金额（万元）	签订合同时间	竣工验收报告时间	联系人及电话
1					
2					
3					
4					
...					

根据上述业绩情况，按招标文件要求附销售或服务合同复印件及评审标准要求的证明材料。

格式十七：

《技术和服务要求响应表》

序号	标的名称	参数性质	采购文件规定的技术和 服务要求	投标文件响应的 具体内容	型号	是否偏离	证明文件所在位 置	备 注
1								
2								
3								
4								
5								
6								
...								
...								

说明：

- 1.“采购文件规定的技术和服务要求”项下填写的内容应与招标文件中采购需求的“技术要求”的内容保持一致。投标人应当如实填写上表“投标文件响应的具体内容”处内容，对采购文件提出的要求和条件作出明确响应，并列明具体响应数值或内容，只注明符合、满足等无具体内容表述的，将视为未实质性满足招标文件要求。投标人需要说明的内容若需特殊表达，应先在本表中进行相应说明，再另页应答，否则投标无效。
2. 参数性质栏目按招标文件有标注的“★”、“▲”号条款进行填写，打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。打“▲”号条款为重要技术参数（如有），若有部分“▲”条款未响应或不满足，将根据评审要求影响其得分，但不作为无效投标条款。
3. “是否偏离”项下应按下列规定填写：优于的，填写“正偏离”；符合的，填写“无偏离”；低于的，填写“负偏离”。
- 4.“备注”处可填写偏离情况的说明。

格式十八：

《商务条件响应表》

序号	参数性质	采购文件规定的商务条件	投标文件响应的具体内容	是否偏离	证明文件所在位置	备注
1						
2						
3						
4						
5						
6						
7						
8						
9						
.....						

说明：

1. “采购文件规定的商务条件”项下填写的内容应与招标文件中采购需求的“商务要求”的内容保持一致。
2. 投标人应当如实填写上表“投标文件响应的具体内容”处内容，对采购文件规定的商务条件作出明确响应，并列明具体响应数值或内容，只注明符合、满足等无具体内容表述的，将视为未实质性满足招标文件要求。投标人需要说明的内容若需特殊表达，应先在本表中进行相应说明，再另页应答，否则投标无效。
3. 参数性质栏目按招标文件有标注的“★”、“▲”号条款进行填写，打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。打“▲”号条款为重要技术参数（如有），若有部分“▲”条款未响应或不满足，将根据评审要求影响其得分，但不作为无效投标条款。
4. “是否偏离”项下应按下列规定填写：优于的，填写“正偏离”；符合的，填写“无偏离”；低于的，填写“负偏离”。
5. “备注”处可填写偏离情况的说明。

格式十九：

（以下格式文件由供应商根据需要选用）

履约进度计划表

序号	拟定时间安排	计划完成的工作内容	实施方建议或要求
1	拟定__年__月__日	签订合同并生效	
2	__月__日—__月__日		
3	__月__日—__月__日		
4	__月__日—__月__日	质保期	

格式二十：

（以下格式文件由供应商根据需要选用）

各类证明材料

- 1.招标文件要求提供的其他资料。
- 2.投标人认为需提供其他资料。

格式二十一：

采购代理服务费支付承诺书

致：广东志正招标有限公司

如果我方在贵采购代理机构组织的广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）招标中获中标（采购项目编号：ZZ0260087），我方保证在收取《中标通知书》时，按招标文件对代理服务费支付方式的约定，承担本项目代理服务费。

我方如违约，愿凭贵单位开出的违约通知，从我方提交的投标保证金中支付，不足部分由采购人在支付我方的中标合同款中代为扣付；以投标担保函（或保险保函）方式提交投标保证金时，同意和要求投标担保函开立银行或担保机构、保险保函开立的保险机构应广东志正招标有限公司的要求办理支付手续。

特此承诺！

投标人法定名称（公章）：_____

投标人法定地址：_____

投标人授权代表（签字或盖章）：_____

电 话：_____

传 真：_____

承诺日期：_____

格式二十二：

（以下格式文件由供应商根据需要选用）

需要采购人提供的附加条件

序号	投标人需要采购人提供的附加条件
1	
2	
3	

注：投标人完成本项目需要采购人配合或提供的条件必须在上表列出，否则将视为投标人同意按现有条件完成本项目。如上表所列附加条件含有采购人不能接受的，将被视为投标无效。

格式二十三：

（以下格式文件由供应商根据需要选用）

询问函、质疑函、投诉书格式

说明：本部分格式为投标人提交询问函、质疑函、投诉函时使用，不属于投标文件格式的组成部分。

询问函

广东志正招标有限公司

我单位已登记并准备参与“广东省国土资源技术中心政务信息化运维（2026年）项目（基础设施及运行维护服务）”项目（采购项目编号：ZZ0260087）的投标活动，现有以下几个内容（或条款）存在疑问（或无法理解），特提出询问。

- 一、_____（事项一）
 - （1）_____（问题或条款内容）
 - （2）_____（说明疑问或无法理解原因）
 - （3）_____（建议）
- 二、_____（事项二）
- ...

随附相关证明材料如下：（目录）

询问人（公章）： _____
法定代表人或授权代表（签字或盖章）： _____
地址/邮编： _____
电话/传真： _____

日期： 年 月 日

质疑函

一、质疑供应商基本信息

质疑供应商：

地址：_____ 邮编：_____

联系：_____ 联系电话：_____

授权代表：_____

联系电话：_____

地址：_____ 邮编：_____

二、质疑项目基本情况

质疑项目的名称：_____

质疑项目的编号：_____ 包号：_____

采购人名称：_____

采购文件获取日期：_____

三、质疑事项具体内容

质疑事项1：_____

事实依据：_____

法律依据：_____

质疑事项2：_____

.....

四、与质疑事项相关的质疑请求

请求：_____

签字(签章)：_____ 公章：_____

日期： 年 月 日

质疑函制作说明：

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体采购包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

投诉书

一、投诉相关主体基本情况

投诉人：_____

地 址：_____ 邮编：_____

法定代表人/主要负责人：_____

联系电话：_____

授权代表：_____ 联系电话：_____

地 址：_____ 邮编：_____

被投诉人1：_____

地址：_____ 邮编：_____

联系人：_____ 联系电话：_____

被投诉人2：_____

.....

相关供应商：_____

地址：_____ 邮编：_____

联系人：_____ 联系电话：_____

二、投诉项目基本情况

采购项目名称：_____

采购项目编号：_____ 包号：_____

采购人名称：_____

代理机构名称：_____

采购文件公告:是/否 公告期限：_____

采购结果公告:是/否 公告期限：_____

三、质疑基本情况

投诉人于____年____月____日,向提出质疑, 质疑事项为：_____

采购人/代理机构于____年____月____日,就质疑事项作出了答复/没有在法定期限内作出答复。

四、投诉事项具体内容

投诉事项 1：_____

事实依据：_____

法律依据：_____

投诉事项2：_____

.....

五、与投诉事项相关的投诉请求

请求：_____

签字(签章)：_____ 公章_____

日期：____年____月____日

投诉书制作说明：

1.投诉人提起投诉时，应当提交投诉书和必要的证明材料，并按照被投诉人和与投诉事项有关的供应商数量提供投诉书副本。

2.投诉人若委托代理人进行投诉的，投诉书应按要求列明“授权代表”的有关内容，并在附件中提交由投诉人签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

- 3.投诉人若对项目的某一分包进行投诉，投诉书应列明具体分包号。
- 4.投诉书应简要列明质疑事项，质疑函、质疑答复等作为附件材料提供。
- 5.投诉书的投诉事项应具体、明确，并有必要的事实依据和法律依据。
- 6.投诉书的投诉请求应与投诉事项相关。
- 7.投诉人为自然人的，投诉书应当由本人签字；投诉人为法人或者其他组织的，投诉书应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

格式二十四：

（以下格式文件由供应商根据需要选用）

项目实施方案、质量保证及售后服务承诺等内容和格式自拟。

格式二十五：

附件（以下格式文件由供应商根据需要选用）

政府采购投标（响应）担保函

编号：【 】号

（采购人）：

鉴于_____（以下简称“投标（响应）人”）拟参加编号为_____的（以下简称“本项目”）投标（响应），根据本项目采购文件，投标（响应）人参加投标（响应）时应向你方交纳投标（响应）保证金，且可以投标保险凭证的形式交纳投标（响应）保证金。应投标（响应）人的申请，我方以保险的方式向你方提供如下投标保证保险凭证：

一、保险责任的情形及保证金额

（一）在投标（响应）人出现下列情形之一时，我方承担保险责任：

- 1.中标（成交）后投标（响应）人无正当理由不与采购人签订《政府采购合同》；
- 2.采购文件规定的投标（响应）人应当缴纳保证金的其他情形。

（二）我方承担保险责任的最高金额为人民币_____元（大写）即本项目的投标（响应）保证金金额。

二、保证的方式及保证期间

我方保证的方式为：连带责任保证。

我方的保证期间为：本保险凭证自__年__月__日起生效，有效期至开标日后的90天内。

三、承担保证责任的程序

- 1.你方要求我方承担保证责任的，应在本保函保证期间内向我方发出索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的账号、户名和开户行，并附有证明投标（响应）人发生我方应承担保证责任情形的事实材料。
- 2.我方在收到索赔通知及相关证明材料后，在15个工作日内进行审查，符合应承担保证责任情形的，我方按照你方的要求代投标（响应）人向你方支付相应的索赔款项。

四、保证责任的终止

- 1.保证期间届满，你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。
- 2.我方按照本保函向你方履行了保证责任后，自我方向你方支付款项（支付款项从我方账户划出）之日起，保证责任终止。
- 3.按照法律法规的规定或出现我方保证责任终止的其它情形的，我方在本保函项下的保证责任终止。

五、免责条款

- 1.依照法律规定或你方与投标（响应）人的另行约定，全部或者部分免除投标（响应）人投标（响应）保证金义务时，我方亦免除相应的保证责任。
- 2.因你方原因致使投标（响应）人发生本保函第一条第（一）款约定情形的，我方不承担保证责任。
- 3.因不可抗力造成投标（响应）人发生本保函第一条约定情形的，我方不承担保证责任。
- 4.你方或其他有权机关对采购文件进行任何澄清或修改，加重我方保证责任的，我方对加重部分不承担保证责任，但该澄清或修改经我方事先书面同意的除外。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为 法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：_____（公章）_____

联系人：_____

联系电话：_____

____年__月__日

格式二十六：

政府采购履约担保函

编号：

（采购人）：

鉴于贵方在_____项目（项目编号为_____以下简称“项目”）的采购中，确定_____为中标人/供应商，拟签订/已签订项目相关采购合同（以下简称“主合同”）。依据主合同的约定，供应商应向贵方交纳履约保证金，且可以履约担保函的形式交纳履约保证金。应供应商的申请，我方以保证的方式向贵方提供如下履约保证金担保：

一、保证金额

我方的保证范围是主合同约定的合同价款总额的_____%，数额为_____（大写），币种为人民币（即主合同履约保证金金额）。

二、我方保证的方式为：连带责任保证。

三、我方保证的期间为：本保函自开立之日起生效，至 年 月 日止。

四、在本保函的有效期内，如被保证人违反上述合同或协议约定的义务，我方将在收到你方提交的本保函文件及符合下列全部条件的索赔通知后 30 个工作日内以上述保证金额为限支付你方索赔金额：

（一）索赔通知文件必须以书面形式提出，列明索赔金额，并由你方法定代表人(负责人)或授权代理人签字并加盖公章；

（二）索赔通知文件必须同时附有：

1. 一项书面声明，声明索赔款项并未由被保证人或其代理人直接或间接地支付给你方；

2. 证明被保证人违反上述合同或协议约定的义务以及有责任支付你方索赔金额的证据。

（三）索赔通知文件必须在本保函有效期内到达以下地址：

_____。

五、本保函保证金额将随被保证人逐步履行保函项下合同约定或法定的义务以及我方按你方索赔通知文件要求分次支付而相应递减。

六、本保函项下的权利不得转让，不得设定担保。受益人未经我方书面同意转让本保函或其项下任何权利，我方在本保函项下的义务与责任全部消灭。

七、本保函项下的合同或基础交易不成立、不生效、无效、被撤销、被解除，本保函无效；被保证人基于保函项下的合同或基础交易或其他原因的抗辩，我方均有权主张。

八、因本保函发生争议协商解决不成，按以下第（一）种方式解决：

（一）向我方所在地的人民法院起诉。

（二）提交 此栏空白 仲裁委员会(仲裁地点为此栏空白)按照申请仲裁时该会现行有效的仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。

九、本保函适用中华人民共和国法律。

十、其他条款：

1. 本保函有效期届满或提前终止，本保函自动失效，我方在本保函项下的义务与责任自动全部消灭，此后提出的任何索赔均为无效索赔，我方无义务作出任何赔付。

2. 所有索赔通知必须在我方工作时间内到达本保函规定的地址。

十一、本保函自我方盖章之日起生效。

保证人：_____（盖章）

联系地址：_____

联系电话：_____

开立日期：__年__月__日

采购合同履行保险凭证

致被保险人_____：

鉴于你方_____（招标方/被保险人）接受投保人_____（投标方）参加_____（采购）项目的投标，向投保人签发中标通知书，投保人在我公司投保《采购合同履行保证保险》，我公司接受投保人的请求，在保险责任范围内，愿意就投保人履行与你方订立的采购合同，向你方提供如下保证保险：

一、我公司对上述采购项目出具的《采购合同履行保证保险》保单号：

二、上述保单项下我公司的保险金额（最高限额）：人民币（¥：元）

上述全部保险单的保险金额随投保人逐步履行采购合同约定的义务或我公司的赔付而递减。

三、本保险的保险期间自____年__月__日__时起至____年__月__日__时止，共计__天。

四、本保险合同仅承担履约保证责任：在本保险期限内，供应商在《采购合同》的履约过程中，因下列情形给你方造成直接损失的，在收到你方提交的符合保险合同约定的全部条件的书面文件，我公司依据保险合同有关约定并与你方达成一致赔偿意见后 30 个工作日内以上述保险金额为限，支付你方索赔金额。

（一）投保人未按照采购合同约定的时间、地点交付采购标的；

（二）投保人供应采购标的的规格、型号、数量、质量等不符合《采购合同》的约定。

五、索赔文件

（一）经被保险人有权人签字、加盖被保险人公章的书面索赔声明正本，索赔声明须注明本保险凭证对应的保单号并申明如下事实：

（1）投保人未履行采购合同相关义务；

（2）投保人的违约事实。

（二）保险单正本；

（三）《采购合同》副本及与采购项目进展、质量、缺陷有关的证明文件（包括《中标通知书》、投标书及其附录、会议纪要、其他合同文件等）；

（四）保险人要求投保人、被保险人所能提供的与确认保险事故的性质、原因、损失程度等有关的其他证明和资料；

（五）仲裁机构出具的裁决书或法院出具的裁定书、判决书等生效法律文书（适用于仲裁或诉讼确认损失的方式）；

六、未经保险人书面同意，本保险凭证与保险合同不得转让、质押，否则保险人在本保险凭证与保险合同项下的保险责任自动解除。

七、本保证保险发生争议协商解决不成，向保险人所在地有管辖权的人民法院提起诉讼。

八、本保证保险适用的保险条款为《_____》。

九、保险责任免除及其他本保险凭证未载明事宜以保险合同约定为准。

十、本保险凭证自保险人加盖保单专用章起生效。

保证人：_____（盖章）

地址：_____

电话：_____

开立日期：____年__月__日