项目编号：510101202101706

成都市城市管理数字化监督管理中心
成都市数字化城市管理信息系统2021-2022年度运维服务项目

采

购

需

求

四川·成都

成都市城市管理数字化监督管理中心

四川中泽盛世招标代理有限公司

共同编制

二〇二一年十一月

采购项目技术、服务内容及其他商务要求

一、项目概况

成都市数字化城市管理信息系统 2021~2022 年度运维服务项目的运维目标要充分利用专业应用管理、运维服务机构的专业技术水平、人才储备以及丰富的经验，提升数字城管系统的应用水平，维护效率，降低运行管理成本，解决系统应用管理、运行维护任务繁重与专业人才不足之间的矛盾。

建立健全规范科学的运维保障制度，切实保障各项设施设备和系统的安全、稳定、高效的运行，提高系统应用水平，保障数字化城市管理业务高效开展，数据交换准确、完整、及时。为系统后期系统功能优化、改善、升级奠定基础。做到日常有巡检、问题有响应、故障有应急、重大保障有值守。

具体包括但不限于如下内容：

（1）确保系统软件的稳定性、可靠性、安全性和可恢复性；

（2）确保系统故障发生时能得到及时响应与修复；

（3）确保系统的可靠高效运转，强化重大活动时的现场保障；

（4）对数字城管系统的应用、运行进行管理，保障系统基础数据的准确性，业务数据合理性，数据交换完整性、及时性；

（5）配合完成信息安全等级保护（三级）安全相关工作。

本次运维工作将围绕数字城管系统开展系统驻场保障服务和专项支撑服务，主要是对系统进行日常巡检包含：功能、数据库、服务器、接口等，其次提供驻场服务开展用户权限配置、业务需求评估、地理数据更新、接口维护、问题收集处理等工作，建立故障应急机制，及时对系统重大故障进行处理。在重要保障期间派人现场值守，并且后方提供相应的支撑人员支撑突发事件解决等方面的进行日常运行维护工作，并围绕等级保护三级标准开展系统的数据库审计、日志审计等审计工作，系统运行按照系统有关安全制度进行。在等保测评期间配合测评单位及上级部门发布的安全问题对系统的安全缺陷进行整改，并对系统现有政务云安全增值服务（态势感知）进行续约，满足系统等级保护三级要求。

二、现状分析

1、信息系统现状分析

（1）系统建设情况

成都市数字化城市管理信息系统经 2013 年核心数据平台扩容、2015 年系统全面优化升级改造、2018 年系统实现成都市政务云部署和 2019 年全市 22 个区（市）县集中部署使用。并在 2020 年 7 月经市公安局定级为等保三级，同年 11 月完成定级备案工作。集中部署服务合同于 2021 年 10 月（满足验收要求的情况下）结束。

（2）系统功能情况

数字城管系统共 22 个子系统，其中基础子系统 9 个，拓展子系统 13 个。各子系统部署于相同环境，采用操作系统、中间件及功能组件相同，具体见下表：

表 2-1 功能清单

序号	子系统名称	操作系统	中间件	功能组件
1	无线数据采集系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
2	监督中心受理子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
3	协同工作子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
4	监督指挥子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
5	综合评价子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
6	基础数据管理子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
7	应用维护子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
8	地理编码子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
9	数据交换子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
10	城乡环境综合治理问题库子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
11	监督检查子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
12	视频监控子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
13	部件在线更新子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
14	移动督办子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0

序号	子系统名称	操作系统	中间件	功能组件
15	短信平台子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
16	移动处置子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
17	专项普查子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
18	智慧城管综合应用APP	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
19	车载信息采集子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
20	多维分析子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
21	空间分析子系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0
22	信息采集工作监督管理系统	Centos7.5	apache-tomcat-7.0.85	nginx1.14.0

（3）系统运行情况

数字城管系统从2020年4月27日开始在成都市22个区（市）县试运行，截止2020年10月31日，共上报案件2105507条，其中立案数为2095284条，处置数为1770944条，结案数为1769725条。系统试运行期间，郊区市县共反馈问题140个，已处理140个。

目前系统注册账号约为：5669,日活跃用户约为：1700。通过集中部署工作收集到的用户提出问题，如：账号无法登录、账号缺失、考核指标有误、智信APP不能定位等情况。系统各功能模块运行及健康状态总体良好。

（4）上云情况

数字城管系统云服务商为浪潮云。基础运行环境包括：

服务器（共25台，用于部署系统应用、arcgis以及数据库集群）

云存储（共65T，15T分配给各服务器，50T用于多媒体数据存储）

网络（1个政务网地址，1个互联网地址）

互联网：http://171.221.172.74:6888/eUrbanMIS

政务网：http://10.1.235.35:6888/ eUrbanMIS

操作系统（共25个，5个Windows Server 2012 64位，20个Linux Centos 7.5）

应用安全工具（共 27 个，1 个虚拟 web 防火墙，1 个虚拟防火墙，25 个防病毒工具）

表 2-2 浪潮云资源清单

浪潮云资源单				
资源类型	资源描述		数量	说明
云服务器	标准型 C	8 核/16GB 内存/160GB 硬盘	20	应用服务器 1-9、无线服务器 1-4、多媒体服务器、对接服务器 1-2、预发布服务器 1-4
	标准型 E	16 核/32GB 内存/160GB 硬盘	2	GIS 服务器 1、GIS 服务器 2
物理服务器	增强 A 型	2*10 核/256G 内存/4*600G(SAS)硬盘	1	视频图像处理，需配置 GPU 显卡
	增强 B 型	4*18 核/512G 内存/4*600G(SAS)硬盘	2	Mysql 数据库集群
云存储	光纤存储、数据库存储（单位：TB）		4T	2 台增强 B 型服务器每台分配 2T 用于数据存储
	分布式存储、文件存储（单位：TB）		61T	50T 用于多媒体数据存储；11T 平均每台服务器分配 0.5T 用于存储数据
网络	电子政务外网	IP 地址数量	1	
	互联网	电信 IP 地址数量	共享 1	
操作系统	Windows Server 2012 64 位		4	2 台 GIS 服务器、2 台对接服务器
	主流 Linux		21	Centos7.5
应用安全工具	虚拟 web 防火墙		1	2021 年 10 月 11 日到期
	虚拟防火墙		1	
	虚拟 IDS		1	

	防病毒	25	
	态势感知	25	2021 年 10 月 11 日到期
	数据库审计	2	
	日志审计	25	

表 2-3 服务期资源清单

服务器名称（含操作系统）	服务器 ip	说明
应用服务器		
应用服务器 1（centos 7.5）	172.25.43.167	Imserver（8081）、geoserver（8081）、MIS（6666）、主服务 nignx（6888）
应用服务器 2（centos 7.5）	172.25.43.168	MIS（6666）、GIS（6777）、智信主服务 nginx（6888）
应用服务器 3（centos 7.5）	172.25.43.169	MIS（6666）、GIS（6777）、gis 服务 nginx（6888）
应用服务器 4（centos 7.5）	172.25.43.177	MIS 服务对接（6888）、天地图 nginx 缓存（6777）、车载服务（6888）
应用服务器 5（centos 7.5）	172.25.43.178	MIS（6666）、GIS（6888）
应用服务器 6（centos 7.5）	172.25.43.180	运维监控
应用服务器 7（centos 7.5）	172.25.43.181	MIS（6666）、GIS（6888）
应用服务器 8（centos 7.5）	172.25.43.182	MIS（6666、GIS（6888）
应用服务器 9（centos 7.5）	172.25.43.183	MIS（6666）、GIS（6888）
数据库服务器		
业务库（centos 7.5）	172.25.43.159	业务库主
业务库从（centos 7.5）	172.25.43.170	业务库从
业务库从（centos 7.5）	172.25.43.171	业务库从
业务库从（centos 7.5）	172.25.43.172	业务库从
业务库从（centos 7.5）	172.25.43.173	业务库从
统计库（centos 7.5）	172.25.43.160	统计库主

统计库从（centos 7.5）	172.25.43.175	统计库从

2、运维服务现状分析

数字城管系统于2019年12月部署于成都市政务云浪潮云上，支持成都市电子政务外网和互联网访问，集中部署项目服务期至2021年10月（正常服务情况下），2021年10月后集中部署项目服务完成，集中部署项目不再提供后续运维服务。

（三）服务需求

经2019年成都市数字化城市管理信息系统集中部署服务项目后数字城管系统实现了全成都市的全市部署，22个区（市）县停止使用自建数字城管系统，实现全市数字城管系统集中部署达到全市数字城管系统标准统一、流程统一、功能统一、数据统一、环境统一的目的。

本次系统的运维工作关乎提升全市城市管理业务的流转效率和数字化城市管理信息系统的运行效率，维持城市管理问题处置的自动化和快速化，管理评价考核的全面化和科学化，进一步促进和完善“统一指挥、监督有力、沟通快捷、分工明确、责任到位、反应快速、处置及时、运转高效”的城市管理机制，不断提升公共服务质量和水平，为市民提供快速、优质、高效的城市管理综合服务。

严格做好系统的日常运行巡检工作，按照不同的频次对系统功能、服务器、数据库、数据推送情况。并每日向采购单位负责人提交书面巡检表。有重大隐患或故障需及时汇报采购单位负责人，评估其影响及完成处理时限。

1、驻场保障服务

驻场服务为保障数字城管系统共 22 个子系统，其中基础子系统 9 个，拓展子系统 13 个（具体见附件功能点清单），约 210 个功能点正常运行，通过 QQ 群、电话等渠道收集系统用户反馈问题，收集到问题后，需要运维单位根据不同类别的问题，进行相应的流程进行审批。开展每日系统巡检、用户管理、数据备份、文档报告编写、业务需求评估、接口可用、接待保障、竞赛系统搭建、客服服务、技术支撑等工作。

2、专项支撑服务

（1）故障应急

系统每年有约 30 次系统参观、演示、保障工作，以及为保障系统出现故障后，通过流程化及预防系统因故障而对业务工作开展造成巨大的影响，建立相应

的故障应急机制，最大限度减轻。实现各应用场景下，数字城管系统的正常运行，应安排现场运维工程师现场值守，后台应安排技术工程师保障平台功能和服务器的正常运行，如果平台出现故障，按故障处理服务流程进行处理；在重要值守期间接受采购单位的工作安排。

（2）地理数据更新

用户单位每年会不定期对成都市地理普查数据进行更新。为保障普查成果在业务工作中得以应用，不断提升数字城管系统的用户提验，运维单位须将业主单位提供的更新后的地理编码数据进行测试并更新到系统。

（3）信息安全管理

数字城管系统 2020 年 10 月通过了系统的三级等保测试整改工作，按照三级等保有关要求制定了安全制度，要求对系统、数据、账号等进行安全管理，及时发现潜在的安全问题。

（4）信息安全整改工作

信息安全服务数字城管系统在 2020 年经网络安全相关部门定级为等级保护三级系统，按照国家有关的政策文件要求，等级保护三级系统每年至少进行一次等级测评工作，为落实国家相关法律法规和制度要求，满足相关主管单位和行业要求，在本项目运维期间仅需提供相应的信息安全服务使系统的运行满足三级等保的运行标准，并对等级保护测试中发现的信息安全问题进行整改，城管委会不定期对委内系统进行安全扫描等安全服务，在收到有关整改要求后及时对安全问题进行整改。

政务云安全产品态势感知。在 2020 年度的系统等级保护三级测试中，第三方测试单位依据《信息安全技术网络安全等级保护基本要求》（GB / T 22239-2019）对成都市数字化城市管理信息系统实施了网络安全等级保护测评，测评结果表明成都市数字化城市管理信息系统存在高危安全漏洞，系统存在的高风险问题 7 个，其中 5 个通过软件完善优化及中心安全制度的制定得以解决，另外两个分别为：一是通过对应用系统实施渗透测试表明系统存在 SQL 注入、XSS、文件上传、弱口令、明文传输等高危安全漏洞；二是电子政务外网边界无法实现对应用层面的安全防护，在电子政务外网和互联网边界上均缺少对 APT 新型攻击的防御能力。此两个高危漏洞不能通过系统软件优化完善得以解决。

为使成都市数字化城市管理信息系统能够满足等级保护三级的要求，中心配备态势感知和云 WAF 设备，加强系统网络边界的防护，保障成都市数字化城市管理信息系统的安全运行。在 2020 年度中心要求服务单位响应了测试单位整改要求，向政务云（浪潮）购买了为期一年的云 Waf 和态势感知服务，满足三级等保要求，系统通过了等级保护测试。

经调研，本次运维年度中，政务云（浪潮）云 Waf 部署范围已满足等级保护三级要求。遂本次运维年度不再购买云 Waf 服务，由于政务云基础服务无态势感知服务，为满足系统等级保护三级要求，本次运维年度将继续向政务云采购态势感知服务。

表 2-4 成都市政务云（浪潮）服务目录清单

服务项目	明细	计量单位
计算服务	1G 内存	GB·月
	1 核 CPU	核·月
物理服务器	裸金属物理服务器 1	台.月
	裸金属物理服务器 2	台.月
	裸金属物理服务器 3（大数据处理节点）	台.月
存储	分布式存储、文件存储	TB·月
	FC 存储（通用块存储）	TB·月
	FC 存储（SSD 块存储）	TB·月
	视频云存储	100TB.月
linux 系统	提供主流版本 linux 操作系统	套·月
应用安全	虚拟 web 防火墙	实例.月
	虚拟防火墙	实例.月
	虚拟 IDS	实例.月
	防病毒	实例.月
	安全审计	实例.月
	提供应用负载均衡服务	实例.月
高性能计算	基于 Intel V4 架构处理器提供计算能力，CPU 主频不少于 2.4GHz，平台 CPU 核心数不少于 384 核，并	核时

	使用 56Gb Infiniband 高速网络组网。全年最少可提供核时数为 365 天*8 小时*384 核=1121280 核时	
设备托管	设备托管	U.月 机柜·月
光纤链路租用费用	云服务平台互联裸光纤链路	对.公里.月
国产数据库	提供自主可控的国产数据库	套.月
用户培训	提供政务云技术交流培训服务	次
网络	管理网络、业务网络、存储网络、网出口网络等	项·年
平台安全	防火墙、IDS、防火墙、行为审计、漏洞扫描、流量清洗等安全设备，防病毒软件及 APM 应用系统性能管理服务等。	项·年
机房	A 类机房	项·年
运维服务	含政务云运行维护、应用系统上云配合等服务	项.年

（四）服务要求

1、运维服务清单

表 3-1 运维服务清单

序号	服务名称	服务子项	内容概述
1	驻场服务	每日系统巡检	每天 2 次定时对 9 大基础子系统功能模块进行巡检；每周不少于 2 次对以下扩展子系统进行巡检；每周不少于 1 次对以下扩展子系统功能进行巡检；每日对服务器资源使用情况进行监控，包括 CPU、内存、存储等； 对巡检发现的问题及时进行排查处置，根据巡检情况实时增加巡检内容并根据巡检情况形成书面的巡检记录。
		用户管理	根据业务需求，及时根据各区（市）县提交的书面需求单对系统用户进行调整，如：账号名称和密码

			变更（新增、删除和修改）、监督员责任网格调整、专业部门账号调整、账号权限变更等。每月不少于 1 次定期将系统内的测试账号、无用账号进行清理。
		数据备份工作	建立每日备份机制，对业务数据库和统计数据库每天进行备份。每日对前一天备份文件进行检查，确保数据库完全备份成功。另外还需配合灾备公司完成系统数据库、多媒体的灾备工作，当系统备份存在异常，配合灾备公司对故障原因进行排查并及时解决。
		文档类工作	按照业主单位要求定期出具系统运维月报、季度报告等。
		用户的业务需求评估	协助业主单位对收集到的系统用户需求从技术上、业务上进行评估。
		接口维护	根据采购方的对接需求，对现有 9 个的外部系统对接接口的可行性、系统稳定性进行日常维护；
		系统接待保障工作	按照业主要求，做好接待保障工作。接待前及接待当天，重点对系统功能及系统运行情况（包括应急系统）进行自查，确保接待工作顺利进行。
		竞赛系统搭建、维护	按照中心业务要求，每年中心将组织各区（市）县、市级采集公司、市级平台公司等开展业务竞赛。服务单位应按照业务需求搭建竞赛系统，实现竞赛系统中案件上报、受理、立案、派遣、处置、督查、核查和结案流程正常，并能够对数据进行统计分析。
		网络攻防演练	配合业主单位完成网络安全攻防演练工作，对第三方的攻防演练方案进行评估，并出具相对应的防守方案。演练完成后及时总结经验出具演练报告。协调有关的安全厂商及政务云技术人员配合演练，在演练前，根据防守方案做好相关准备工作。
		客服服务	运维单位与各用户单位建立即时通讯渠道，实时的

			收集用户在系统使用期间发现的问题，向用户解答操作。安排技术人员在数字城管系统日常运行时间，在采购单位安排的办公地点安排人员驻场，对系统用户在使用过程中发现的问题，对系统运行中出现的用户问题进行现场处理，并建立统一的问题记录平台，方便对问题的处理过程进行跟踪、督查向用户实时的反馈问题记录、分析、诊断、处理进度等情况，运维单位指定后端专门的支撑人员和管理团队解决驻场人员不能解决的问题，并在故障处理完成后向反映问题用户确认问题解决情况。每月统计用户反映频率较高的故障，按故障类型提供系统功能及操作指导、常见问题解答、异常现象的分析与解答等手册，定期更新，并定期向用户提交报告。确保数字城管系统主要业务工作能及时恢复运行。
2	保障支撑服务信息安全服务	故障应急	针对系统的运行情况对系统进行应急演练，并在系统出现重大故障时，按照预设的处理流程，及时汇报给用户单位相关联系人，并执行预案中要求运维单位处理的相关事项。根据采购单位的实际需求，提供针对重要事件、重要时段、突发事件等特殊时段的现场技术值守，提高对突发事件的响应速度与处理时效，从而有力的保障业务工作的正常运作。
		重点值守保障	重点保障值守期间，运维团队应全面保障数字城管系统各应用场景下的技术操作和运行保障，保障团队应包含运维工程师、支撑工程师等经验丰富的运维人员。
		地理数据更新	根据用户单位需求，每年会不定期对成都市地理数据进行更新。运维单位须将业主单位提供的更新后的地理编码数据进行测试并更新到系统。
		信息安全管理	进行安全设备日常管理，数据库审计、日志审计、

			态势感知、防火墙等设备日志分析、威胁发现等
		配合等保测试整改	配合系统的三级等保测试进行相应的整改。
		网络攻防演练	配合业主单位完成网络安全攻防演练工作，对第三方的攻防演练方案进行评估，并出具相对应的防守方案。在及时协调各方资源完成演练防守，确保顺利完成演练。演练完毕后，根据实际的演练结果出具报告给业主单位。

2、运维对象清单

本次运维系统数字城管系统部署于成都市政务云浪潮云上，接入电子政务外网和互联网。运维服务不包含基础设施部分，数字监管中心网络及基础设施设备已由单独的运维服务进行维护，各区（市）县的网络及基础设施设备由各区（市）县自行维护。

3、运维服务内容及要求

本项目服务内容在 ITSS 运维通用要求的基础上，根据项目特色，围绕以下内容进行运维工作。运维单位及时获得运行维护服务对象状态，发现并处理潜在的故障隐患。并在接到采购单位服务请求或故障申告后，尽快降低和消除对需方业务的影响。在运维服务的过程中为适应采购单位业务要求，通过提供调优改进服务，达到提高运行维护服务对象性能或管理能力的目的，结合需方业务需求，通过对运行维护服务对象的调查研究或分析评价，为采购单位提供报告或建议。

（1）驻场保障服务

★1）数字城管系统运行期间提供驻场服务，现场驻场负责人 1 名；现场驻场技术人员不少于 4 名，且现场驻场负责人与现场驻场技术人员须为不同人员。

2）现场驻场人员需具备进行系统日常巡检、简单系统问题处理等能力。系统全年无休，工作时间夏季（5 月 1 日-10 月 31 日）7:30~22:30，冬季（11 月 1 日-次年 4 月 30 日）7:30~21:30。要求在每日早上 7：30-9：00、17：00-21：30（冬季）/22:30(夏季)，周末及国家法定节假日不少于 1 人；9：00~17：00 提供不少于 2 名工作人员驻场服务并保障 7×24 小时有人响应。**根据《劳动法》第三十六条规定：国家实行劳动者每日工作时间不超过八小时、平均每周工作时间不**

超过四十小时的工时制度。夏季（5.1~10.31）共 184 天，共计工时：[（2+7.5）×1+8×2]×184=4692 小时；冬季（11.1~4.30）共 181 天，共计工时：[（2+6.5）×1+8×2]×181=4434.5 小时；共计工时：9126.5 小时，本年度运维工作服务商约需投入：9126.5÷[（40（小时）×4（周）×12（月）]≈5.0 人。服务期间季度人员更换不超过 1 人次，不可抵抗因素除外。

3）开展每日系统巡检、用户管理、数据备份、文档报告编写、业务需求评估、接口维护、竞赛系统搭建、客服服务、技术支撑等工作。

（2）每日系统巡检

1）每天 2 次定时对 9 大基础子系统功能模块进行巡检，9 大基础子系统包括：无线数据采集子系统、呼叫受理子系统、协同工作子系统、数据交换子系统、地理编码子系统、大屏幕监督指挥子系统、综合评价子系统、应用维护子系统、基础数据资源管理子系统；

2）每周不少于 2 次对以下扩展子系统进行巡检：视频监控子系统、移动督办子系统、短信平台子系统、移动处置子系统、专项普查子系统、智慧城管综合应用 APP、车载信息采集子系统、信息采集工作监督管理系统；

3）每周不少于 1 次对以下扩展子系统功能进行巡检：城乡环境综合治理问题库管理子系统、监督检查子系统、部件在线更新子系统、多维分析子系统、空间分析子系统；

4）每日对服务器资源使用情况进行监控，包括 CPU、内存、存储等；每日系统停用前对外部系统对接接口进行检查，检查内容包括：接口运行情况、已对接完成的数据量与系统是否一致。

对巡检发现的问题及时进行排查处置，并根据巡检情况形成书面的巡检记录。

（3）用户管理

根据业务需求，及时根据各区（市）县提交的书面需求单对系统用户进行调整，如：账号名称和密码变更（新增、删除和修改）、监督员责任网格调整、专业部门账号调整、账号权限变更等。每月不少于 1 次定期将系统内的测试账号、无用账号进行清理。

（4）数据备份工作

建立每日备份机制，对业务数据库和统计数据库每天进行备份。每日对前一

天备份文件进行检查，确保数据库完全备份成功。另外还需配合灾备公司完成系统数据库、多媒体的灾备工作，当系统备份存在异常，配合灾备公司对故障原因进行排查并及时解决。

（5）文档类工作

按照业主单位要求定期出具系统运维月报、季度报告等。

（6）用户的业务需求评估

协助业主单位对收集到的系统用户需求从技术上、业务上进行评估。

（7）接口维护

根据采购方的对接需求，对现有 9 个的外部系统对接接口的可行性、系统稳定性进行日常维护。

（8）系统接待保障工作

按照业主要求，做好接待保障工作。接待前及接待当天，重点对系统功能及系统运行情况（包括应急系统）进行自查，确保接待工作顺利进行。

（9）竞赛系统搭建、维护

按照中心业务要求，每年中心将组织各区（市）县、市级采集公司、市级平台公司等开展业务竞赛。服务单位应按照业务需求搭建竞赛系统，实现竞赛系统中案件上报、受理、立案、派遣、处置、督查、核查和结案流程正常，并能够对数据进行统计分析。

（10）网络攻防演练

配合业主单位完成网络安全攻防演练工作，对第三方的攻防演练方案进行评估，并出具相对应的防守方案。演练完成后及时总结经验出具演练报告。协调有关的安全厂商及政务云技术人员配合演练，在演练前，根据防守方案做好相关准备工作，如：

1）对应用系统存在的漏洞实施修复；对服务器、数据库存在的漏洞补丁进行修复；在电子政务外网边界防火墙部署具备有效防护SQL注入、跨站脚本等各类Web攻击的云WAF设备。

2）检查并删除敏感信息；检查并修改系统内的弱口令；调整密码策略复杂度策略，长度不少于8位，且密码包含：大小写+特殊符号+数字。

3）修改管理账户默认密码，调整密码策略复杂度策略，长度不少于8位，且密码

包含：大小写+特殊符号+数字。

4）调整操作系统、数据库、中间件、业务系统相关账号的密码策略复杂度策略，长度不少于8位，且密码包含：大小写+特殊符号+数字；排查并清除应用的测试账号，防止成为攻击跳板；对数据的存储和传输进行加密。

5）协调政务云安全专家到中心配合进行网络安全攻防演练。

6）协调灾备公司提前做好数据库、多媒体文件的备份工作。

及时协调各方资源完成演练防守，确保能够顺利完成并通过网络安全攻防演练。演练完毕后，根据实际的演练结果出具报告给业主单位。

（11）客服服务

运维单位与各用户单位建立即时通讯渠道，实时的收集用户在系统使用期间发现的问题，向用户解答操作。安排技术人员在数字城管系统日常运行时间，在采购单位安排的办公地点安排人员驻场，对系统用户在使用过程中发现的问题，对系统运行中出现的用户问题进行现场处理，并建立统一的问题记录平台，方便对问题的处理过程进行跟踪、督查向用户实时的反馈问题记录、分析、诊断、处理进度等情况，运维单位指定后端专门的支撑人员和管理团队解决驻场人员不能解决的问题，并在故障处理完成后向反映问题用户确认问题解决情况。每月统计用户反映频率较高的故障，按故障类型提供系统功能及操作指导、常见问题解答、异常现象的分析与解答等手册，定期更新，并定期向用户提交报告。确保数字城管系统主要业务工作能及时恢复运行。

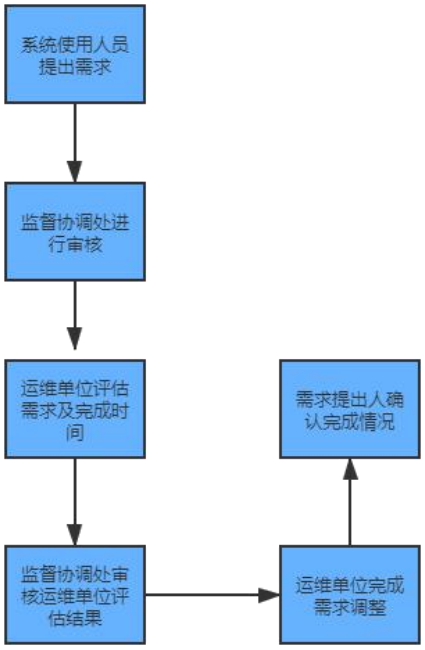

图3-3 账号调整类问题处理流程

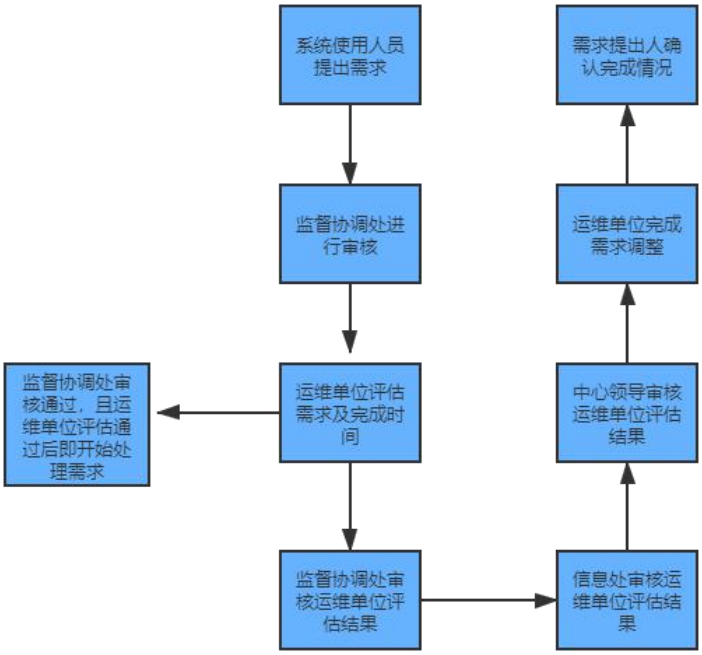

图 3-4 业务调整类问题处理流程

1）受理

①应详细、准确记录反映人、受理时间、反映内容等信息。

②接到电话、邮件、QQ 等 10 分钟内，应完成记录并交办。

③如反映人询问问题解决时间，应根据问题性质告知。

④如咨询方面的问题或电话能直接答复的问题，应直接回复。

⑤结束通话前，应询问是否还需要其他帮助等服务用语。

2）交办

①问题交办前，应根据问题性质及处置要求确定交办时限。

②交办类问题，应在接到 10 分钟内，交办给相应处理人员。

3）回复

①问题解决后，应向反映人回复，反馈过程应做好记录。

②如问题在 3 个工作日内无法处置完毕，应告知反映人处理进度。

4）结案

①应经反映人确认处理结果后结案。

②应定期将结案问题报采购单位。

（12）其它技术支撑工作

按照中心要求，配合外部单位进行成都数字城管系统相关的技术支撑、保障工作，提出技术性的评估意见。

4、专项支撑服务

为实现系统在各种故障突发重大故障场景下驻场人员不能及时分析、查找、解决问题时，业主单位提供的更新后的地理编码数据进行测试并更新到系统。按照有关安全制度要求，需要对系统、数据、账号等进行安全管理，以及按照三级等级保护系统测评要求，每年需要进行一次等级保护测试，运维单位不仅需要进行日常安全运维管理还需要协助采购人开展新一年度的等级保护测试工作，进行对测试问题进行整改。当需要项目团队解决问题时运维服务团队有足够能够及时响应，协助解决。实现各应用场景下，数字城管系统的正常运行。

（1）故障应急

通过运维热线用户反映的情况或系统巡检，及时发现系统异常。在发现系统异常后，应尽快确定故障原因以及影响范围，故障级别在二级以上的，应及时告知数字城管实施机构后方团队。并启动故障应急预案，按图 3-3 及图 3-4 问题处理流程，进入问题交办和跟踪流程。密切跟踪并记录故障处理状态，二级故障以上的，每小时向上级部门通知解决过程和情况。运维单位解决故障问题后，进行

系统测试，确认故障排除。故障级别在三级以上的，在发现故障后，运维管理部门应及时向受影响的数字城管各有关部门和专业部门进行通报。故障处置完毕后，应及时向上述部门进行再次通报。应急处置工作结束后，运维服务运维单位应对事件发生原因、性质、影响、处置过程等进行总结；根据应急处置中暴露出的管理、协调和技术问题，改进和完善预案。运维管理部门在故障结束一周内应向上级部门提交故障处置总结报告。

表 3-5 系统故障等级划分及要求

等级	程度	响应时间	解决时限	通报要求
一级	系统中的关键设备或应用软件出现故障，导致系统瘫痪，重要核心业务无法开展，或出现严重信息、数据出错、重要数据丢失。	5 分钟	自故障申报时起 2 小时内解决。	故障发生后应及时报告运维管理部门，通知受影响的各有关部门和专业部门。 每小时向运维管理部门报告解决进度和情况。
二级	系统中的主要设备或应用软件出现故障，或处理性能严重下降，基本业务受到严重影响。	10 分钟	自故障申报时起 3 小时内解决。	故障发生后应及时报告运维管理部门，通知受影响的各有关部门和专业部门。 每小时向运维管理部门报告解决进度和情况
三级	系统的部分操作性能受损，处理部分性能出现下降，系统功能削弱，但大部分业务运作仍可正常工作。	20 分钟	自故障申报时起 4 小时内解决。	故障发生后和故障处置完毕后，应及时通知受影响的有关部门和各专业部门。
四级	系统中发现有故障隐患的报错，软硬件临时性报错、某个单项功能	30 分钟	自故障申报时起 5 小时内解	故障处置完毕后，应及时通知受影响的有关部门和各专业部门。

	出错需要修复。		决。	

（2）地理数据更新

根据用户单位需求，每年会不定期对成都市地理数据进行更新。运维单位须将业主单位提供的更新后的地理编码数据进行测试并更新到系统。涉及的相关工作如下：

1）在测试环境对更新后的地理数据入库，检查数据是否可用、是否存在问题；

2）测试环境测试无误后，更新到正式环境进行入库；

3）数据入库后，修改地图相关配置，完成区、街道办事处、社区、单元网格和道路单元网格等基础网格数据的信息维护；

4）配置并完成在地图中展示部件分布情况、部件详细信息展示等；

5）完成各系统中部件总数的统计数据更新；

6）地理数据入库后，须对历史案卷进行修复，确保历史案件能够正常进行业务流转，基础数据普查成果入库。

（3）信息安全管理

数字城管系统 2020 年 10 月通过了系统的三级等保测试整改工作，按照有关安全制度要求，需要对系统、数据、账号等进行安全管理，及时发现潜在的安全问题。

1）系统级安全

系统级的安全主要是从操作系统的角度考虑系统安全措施，防止不法分子利用操作系统的一些 BUG、后门取得对系统的非法操作权限。对防火墙、数据库审计、日志审计、态势感知等安全系统软硬件功能检测，每周 1 次。

2）应用审计

应用审计系统负责应用级行为的记录、分析和管理，它可以使系统管理员更好、更准确地了解和掌握应用系统运行情况，及时发现并解决出现的异常情况。

3）数据库安全

根据数据库业务系统情况和数据量等情况，制定相应的数据库巡检方案，参照方案对数据库执行定期巡检，如：数据库表空间占用情况，数据库慢 SQL 情况，数据库备份策略执行情况等，并填写巡检报告，每周 1 次。

4）数据管理

①对所有数字城管案卷信息等核心数据进行的操作，应经采购单位审核；

②核心数据操作应在系统停运期间进行；

③定期对核心数据的使用情况（如案件存储情况，数据库表空间大小等）进行巡检；

④对基础地形图等涉密数据应按保密工作相关要求做好数据保密工作。

（4）信息安全整改工作

此部分工作主要包含：购买政务云浪潮提供的信息安全（态势感知）服务。协助业主单位开展的信息安全三级等级包含测试工作，对上级有关部门发布的安全问题进行有关的整改、测试。包含但不限于以下工作：

1）配合作好系统前期调研工作，提供系统信息：账号、系统架构等；

2）安排专人负责跟进测评工作；

3）对测试缺陷进行整改，如：系统缺陷、安全管理制度，安全设备购买费用（安全产品服务）等，满足等级保护三级要求；

4）配合完成系统定级备案及系统等级保护备案证明的获取；

5）进行上级有关部门发布的安全问题整改及配合整改完成后的复测工作；

6）购买政务云浪潮提供的信息安全（态势感知）服务。

（5）数据灾备

已使用成都市政务灾备平台，后续将继续使用。

（6）短信功能

已使用成都市政务短信平台，后续将继续使用。

（7）邮件功能

本系统不涉及。

（8）身份认证

本系统不涉及。

（9）地理信息

本系统地图应用已使用规划和自然资源局天地图，后续将继续使用。

（10）系统对接

本系统已与市网络理政中心对接。

数据资源目录

表 3-6 市网络理政中心数据资源目录

序号	历史数据资源名称	数据类别	数据内容	对接频率
1	数字化城管网格信息	业务数据	责任网格名称、责任网格 ID、包含单元网格数量、所属区县 ID、所属区县名称	推送到城管委前置机，共对接 1 次
2	数字城管设施部门区域分布信息	地理数据	区域名称、区域设施数量	推送到城管委前置机，共对接 1 次
3	设施展示信息	地理数据	大类名称、小类个数、小类名称、小类数据	推送到城管委前置机，共对接 1 次
4	路灯类设施信息	地理数据	路灯设施个数、所属区域	推送到城管委前置机，共对接 1 次
5	数字城管设施类别分布信息	地理数据	部件大类名称、部件大类数量	推送到城管委前置机，共对接 1 次
6	数字城管设施部门前十名分布信息	地理数据	权属部门名称、小类设施数量	推送到城管委前置机，共对接 1 次
7	数字城管部件 GIS 数据图层信息	地理数据	部件名称、部件标识码、主管部门代码、主管部门名称、权属单位代码、权属单位名称、养护单位代码、养护单位名称、所在单元网格、部件状态、变更上报时间、数据来源、备注	通过优盘拷贝给市网络理政中心

序号	历史数据资源名称	数据类别	数据内容	对接频率
8	数字化城管案卷信息	业务数据	案件时间、案件大类 ID、案件小类 ID、区域 ID、区域名称、上报人员、案件所属万米单元网格 ID、案件所属街道 ID、案件所属责任网格 ID、案件编号 ID、案件位置 X 坐标、案件位置 Y 坐标、处置部门 ID、处置部门名称、当前办理节点名称、办理节点 ID、受理开始时间、案件存档时间、监督员 ID、多媒体信息、立案时间、专业部门处置时间	每天 1 次(23:00 后推送)
9	案件办理经过	业务数据	案件办理节点 ID、案件办理节点名称	每天 1 次(23:00 后推送)
10	路灯问题信息	业务数据	发送到路灯管理处的案卷 ID、案件开始时间、案卷归档时间	每天 1 次(23:00 后推送)
11	道路积水信息	业务数据	案件 ID、上报时间、发生地点、区域、案件坐标、案件多媒体信息、监督员名称、监督员 ID	每天 1 次(23:00 后推送)
12	路灯当日信息	业务数据	当日路灯案件 ID（已立案未结案）、案件上报时间、案件存档时间	每 1 小时推送一次
13	数字城管监督员基本信息	业务数据	监督员名字、监督员 ID、监督员手机号、监督员状态、责任网格 ID、监督员级别（区/县/市）、所属区域名称	每 1 小时推送一次
14	数字城管监督员实时坐标状态信息	业务数据	监督员 ID、监督员坐标 X、监督员坐标 Y、获取时间、当前状态	每 1 小时推送一次
15	监督员在线信息	业务数据	在线监督员 ID、所属区域、姓名、所属责任网格名称、所属责任网格 ID、联系	每半小时推送一次

序号	历史数据资源名称	数据类别	数据内容	对接频率
			方式	
16	当日案件总数信息	业务数据	问题类型 id、问题类型名称 、上报时间、案件 ID、x 坐标、y 坐标	每半小时推送一次
17	当日案件类别信息	业务数据	问题类型 id、问题类型名称 、上报时间、案件大类名称、案件大类 ID	每半小时推送一次
18	当日案件部门分布信息	业务数据	问题类型 id、问题类型名称 、上报时间、主管部门名称、案件 ID	每半小时推送一次
19	当日案件中心城区区域分布信息	业务数据	问题类型 id、问题类型名称 、上报时间、区域名称、案件 ID、x 坐标、y 坐标	每半小时推送一次
20	当日高发类别统计信息	业务数据	问题类型 id、问题类型名称 、上报时间、案件小类，案件 ID	每半小时推送一次
21	当前处置数信息	业务数据	问题类型 id、问题类型名称 、上报时间、当前处置案件 ID、x 坐标、y 坐标	每半小时推送一次

从上表中可以看出，一次性推送的的数据资源目录共 7 项、每天推送一次资源目录共 4 项、每 1 小时推送一次的共 3 项、每半小时推送一次的共 7 项。

表3-7 国家住建部数据资源目录

序号	数据资源名称	数据类别	数据内容	对接评率
1	国家住建部数据对接接口	部件统计数据	部件大类代码、部件大类名称、部件小类代码、部件小类名称、部件数量	一次性推送
2		网格统计数据	行政区划、覆盖面积（单位/平方公里）、单元网格数量、责任网格数量	一次性推送

序号	数据资源名称	数据类别	数据内容	对接评率
3		人员统计数据	行政区、队伍性质、人员类型、人员数量	一次性推送
4		部门数据	行政区、部门代码、部门名称	一次性推送
5		案件来源统计	行政区、信息采集员发现案件数、市民反映案件数、智能发现案件数、其他	每天 1 次(23:00 后推送)
6		案件类别统计	行政区、部件大类案件数、部件小类案件数、事件大类案件数、事件小类案件数	每天 1 次(23:00 后推送)
7		案件状态统计	行政区、上报时间、上报数、立案数、按时结案数、结案数	每天 1 次(23:00 后推送)
8		区域案件统计	行政区、应处置数、处置数、按期结案数、结案数	每天 1 次(23:00 后推送)
9		部门案件统计	行政区、处置部门、应处置数、处置数、按期处置数、返工数	每天 1 次(23:00 后推送)

从上表中可以看出，一次性推送的的数据资源目录共 4 项、每天推送一次资源目录共 5 项。

表3-8 四川省住建厅数据资源目录

序号	数据资源名称	数据类别	数据内容	对接评率
1	四川省省厅数据对接接口	案件基本信息	问题唯一标识、任务号、问题来源 ID、问题来源、问题类型代码、问题类型、大类代码、大类名称、小类代码、小类名称、立案条件代码、立案条件、部件编码、区名称、街道名称、社区名称、单元网格编码、问题状态、位置描述、问题描述、X 坐标、Y 坐标、案件建立时间	每 10 分钟推送 1 次

从上表中可以看出，对接数据为实时推送，每 10 分钟推送 1 次。

表3-9 市城管委数据资源目录

序号	数据资源名称	数据类别	数据内容	对接评率
1	城管委数据对接接口	部件信息	部件标识码、部件名称、经度、纬度、主管部门代码、主管部门名称、权属单位代码、权属单位名称、养护单位代码、养护单位名称信息、所在单元网格、部件状态、初始日期、变更日期、数据来源、备注	使用介质拷贝
2		案件基础信息	案卷标识、任务号、网格编号（单元、责任）、城区编号、社区编号、街道编号、网格名称（单元、责任）、城区名称、社区名称、街道名称、地址描述、X 坐标、y 坐标、部件标号、问题描述、问题类型 id、问题大类 id、问题小类 id、细类 id、案件类型 id、问题类型名称、问题大类名称、问题小类名称、细类名称、案件类型名称、信息来源 id、信息来源名称、急要件标识、急要件原由、上报时间、存档时间、受理时间、立案时间、派遣时间、案件阶段 id、案件阶段名称	每天 1 次(23:00 后推送)
3		案件办理经过	案件标识、操作时间、操作名称、案件阶段 id、案件阶段名称、当前阶段处理员、当前阶段处理意见	每天 1 次(23:00 后推送)
4		责任网格与监督员关系	责任网格 id、责任网格编码、责任网格名称、区域标识、监督员 ID	一次性推送

5		区域信息	区域编号、区域名称、区域域类型、上级编号	一次性推送
6		监督（采集）员信息	监督员 ID、监督员名称、监督员类型 ID、监督员工卡号、所属区域标识、所属区域	一次性推送
7		现场照片（多媒体表）	案卷标识、媒体用途、媒体类型、媒体名称、多媒体地址路径（存放路径）、创建时间	每天 1 次(23:00 后推送)
8		案件类别关系	问题类型 id、问题大类 id、问题小类 id、细类 id、案件类型 id、问题类型名称、问题大类名称、问题小类名称、细类名称、案件类型名称	一次性推送
9		考评结果	案卷标识、案件编号、上报时间、区域 id、区域、街道 id、街道、社区 id、社区、单元网格、单元网格 id、责任网格、责任网格 id、X 坐标、Y 坐标、问题来源 id、问题来源、问题类型 id、问题类型、大类 id、大类、小类 id、小类、细类 id、细类、案件阶段、问题描述、地址描述、问题级别、上报数、监督员上报数、部门级别 id、部门级别名称、作废阶段 id、作废阶段名称、简易流程数、专业部门 id、专业部门、专业部门所属区域 id、专业部门所属区域、管理部门 id、管理部门、处置时间、公众举报登记数、有效上报数、监督员有效上报数、公众有效举报数、核实数、应发核实数、发核实数、待发核实数、应核实数、按期核实数、受理数、待受	每天 1 次(23:00 后推送)

			理数、不予受理数、按时受理数、应立案数、预立案数、按时预立案数、立案数、有效立案数、待立案数、不予立案数、按时立案数、准确立案数、应派遣数、派遣数、待派遣数、按期派遣数、准确派遣数错误派遣数、应处置数、处置数、按期处置数、超期处置数、超期未处置数、按期待处置数、待处置数、应督查数、待督查数、督察数、按期督查数、应发核查数、按时发核查数、发核查数、待发核查数、核查数、按时核查数、应核查数、应结案数、结案数、按期结案数、超期结案数、按期待结案数、超时待结案数、返工数、返工次数、挂账数、作废数、延期数、上报监督员 ID、上报监督员、监督员所属级别 id、监督员所属级别、监督员所属区域 id、监督员所属区域、管理树一层 id、管理树一层、管理树二层 id、管理树二层、管理树三层 id、管理树三层、管理树四层 id、管理树四层、管理树五层 id、管理树五层、背街小巷 id、背街小巷	
10		计时管理信息	系列 ID、活动属性 ID、立案条件、计时区域 ID、时限	一次性推送
11		监督（采集）员轨迹	监督员 ID、上传时间、经度、纬度	每天 1 次(23:00 后推送)
12		机构信息	部门 ID、部门名称、上级 ID、所属区域	一次性推送

13		岗位信息	岗位 ID、岗位名称、所属部门	一次性推送
14		人员信息	人员 ID、人员名称、所属岗位 ID、所属部门 ID、所属区域 ID	一次性推送

从上表中可以看出，一次性推送的数据资源目录共 8 项、使用介质拷贝的数据 1 项、每天推送一次资源目录共 5 项。

表 3-10 成华区数据资源目录

序号	数据资源名称	数据类别	数据内容	对接评率
1	成华区数据对接接口	案件基本信息	案件标识、业务标识、业务名称、唯一标识、任务号、案件显示编号、问题来源标识、问题来源名称、案件类型标识、案件类型名称、问题类型代码、问题类型标识、问题类型名称、大类标识、大类名称、小类标识、小类名称、问题描述、地址描述、部件编码、破坏等级、破等级名称、区标识、区名称、街道标识、街道名称、社区标识、社区名称、网格标识、网格名称、责任网格标识、责任网格名称、位置类型、X 坐标、Y 坐标、观测点 X 坐标、观测点 Y 坐标、观测角度、观测图像名称、观测图像 X 坐标、观测图像 Y 坐标、格网索引、监督员标识、监督员名字、问题等级标识、问题等级名称、核实消息状态标识、核查消息状态标识、案件建立时间、过程开始时间、案件存档时间、案件结束时间、案件截止时间、案件警告时间、案卷时限信息、案卷计时单位、案件处置	每天 1 次(23:00 后推送)

			时限、案件警告时限、案件已用时间、案件剩余时间、案件已用时间字符串、案件剩余时间字符串、最近延期天数、延期天数、案件优先级、案件显示属性、专业部门标识、专业部门名称、专业部门时限信息、专业部门截止时间、专业部门红绿灯、派遣意见、监督员处置标志、监督员考勤标志、需要处理标志、举报信息标识、事发时间、受理时间、立案时间、派遣时间、专业部门处置时间、地图范围、消息标识、已读标识、主办部门、协办部门、主办人、主办人标识集合、主办科室、主办科室标识集合、当前经办人、当前经办处室、所有经办人、经办人标识集、所有经办处室、经办处室标识集合、立案条件标识、立案条件名称、计时区域标识、计时区域名称、急要件标志、急要件原由、最后活动属性标识、最后活动标识、最后更新时间、立案是否超时、派遣是否超时、处置是否超时、督办是否超时、核查是否超时、处置前图片访问链接集合、处置后图片访问链接集合	
2		案件统计信息	案件号、上报数、受理数、立案数、派遣数、核查数、应处置数、处置数、超期处置数、超期未处置数、返工数	每天 1 次(23:00 后推送)

从上表中可以看出，每天推送一次资源目录共2项。

表 3-11 彭州市数据资源目录

序号	数据资源名称	数据类别	数据内容	对接评率
1	彭州市数据对接接口	历史事件信息	问题描述、经度、纬度、问题来源、上报时间、职能事项、所属地址、当前状态（处理中、督查、办案）、上报图片（可以直接访问的图片 url）	每天 1 次(23:00 后推送）
2		事件预警推送	问题描述、经度、纬度、问题来源、上报时间、职能事项、所属地址、当前状态（处理中、督查、办案）、上报图片（可以直接访问的图片 url）	每天 1 次(23:00 后推送）
3		问题来源	监督员自报自处数量、信息采集员上报数量、成都市监督发现数量、视频上报数量、上报数量	每天 1 次(23:00 后推送）
4		当月案件处置信息	上报数量、受理数量、立案数量、派遣数量、处置数量、核查数量、结案数量、结案率	每天 1 次(23:00 后推送）
5		月度高发事件统计	上报数量、受理数量、立案数量、派遣数量、处置数量、核查数量、结案数量、结案率	每天 1 次(23:00 后推送）
6		城市事件运行分析（区域分析）	XX 镇（街道）、上报案件数量、办结案件数量	每天 1 次(23:00 后推送）
7		城市事件运行分析（趋势分析）	月度（近 6 个月）、上报案件数量、办结案件数量	每天 1 次(23:00 后推送）

从上表中可以看出，每天推送一次资源目录共 7 项。

表 3-12 青白江区数据资源目录

序号	数据资源名称	数据类别	数据内容	对接评率
1	青白江区数据对接	数字化城管案卷信息	案件标识、案件建立时间、案件大类 ID、案件小类 ID、监督员 ID、监督员、单元网格 ID、所属街道 ID、责任网格 ID、X 坐标、Y 坐标、处置部门 ID、处置部门名称、当前办理节点名称、办理节点 ID、受理开始时间、案件存档时间、多媒体信息、立案时间、专业部门处置时间、区域 id、区域名称	每天推送 1 次(23:00 后推送)

从上表中可以看出，每天推送一次资源目录共1项。

2.天府市民云

本系统不涉及。

3.行政执法

本系统不涉及。

4.行政审批

本系统不涉及。

5. 与网络理政中心对接技术要求

2020年9月已完成了对接。

（五）运维制度

制度是一种必须共同遵守的行为规范，是保证工作有序开展和任务圆满完成的基础。建立和健全成都市数字化城市管理信息系统维护的各项管理制度，对于维护工作的顺利完成是必需的。

要求运维团队依据以下标准，协助成都市城市管理数字化监督管理中心建立规范、科学、实用的维护制度。

①《成都市电子政务外网使用管理规定》

②ISO/IEC 9001:2008质量管理体系

③ISO/IEC 20000: 2005 IT服务管理体系

④GBT28827.1-2012信息技术服务运行维护第1部分：通用要求

⑤GBT28827.2-2012信息技术服务运行维护第2部分：交付规范

⑥GBT28827.3-2012信息技术服务运行维护第3部分：应急响应规范

⑦ITSS（Information Technology Service Standards）信息技术服务标准。

1、运维制度总则

运维以技术为基础，通过技术保障产品提供更高质量的服务。在服务出现异常时尽可能快速恢复服务，从而保障服务的可用性；同时深入分析故障产生的原因；推动并修复服务存在的问题，同时设计并开发相关的预案以确保服务出现故障是可以高效止损。

第一条 为保障信息系统的良好运行，使运维技术人员工作制度化、流程化、规范化，特制订运维制度。

第二条 运维管理工作总体目标：立足根本促发展，开拓运维新局面。在系统运行推广时期，通过系统基础环境、应用系统的运维，促进信息系统能够稳定可持续性的发展。

第三条 支持信创，自主可控，全面支持信息技术应用创新技术和产品。软件平台全面支持国产化终端接入。数据库、中间件等软件产品原则上选用国产化软件。包括国产Linux操作系统、国产主流数据库系统。

第四条 运维管理制度的适用范围：运维全体人员。

2、运维工作规范

（1）运维操作规范

1.白天一般只进行例行巡检、紧急更新需要经过审批；

2.对不可逆的删除或修改操作，尽量延迟或慢速执行；

3.应对故障要先恢复再排查，无计可施时重启试试；

4.批量操作，需要在测试环境进行演练；

5.一人一次只做一个变更，降低人为失误风险；

6.数据备份任务要监控，并定时检查备份档的有效性；

7.灾难的紧急预案一定要有演练的机制；

8.每个偶然的故障背后都深藏着必然联系，需要找到问题根源。

（2）数据库操作规范

1.白天一般只进行例行巡检；

2.统计数据在只读实例上统计，没有只读实例的话，若需要消耗大量性能，只在夜间进行计算；

3.对大表的变更需要经过审批；

4.变更需要发送通知和报告，保证信息对齐；

5.重大操作要有操作和回滚方案，要双人检验且审批通过；

6.养成日常巡检核心监控属性的习惯、定期对比各数据中心的库表结构是否一致；

7.做好数据库容量规划，做好容量监控；

8.对索引要根据访问类型做战略性规划；

9.定期的性能优化避免业务量突增造成的雪崩；

10.推动业务采用更合适的架构方案。

（六）运行维护保障

1、运维团队及技术支撑能力保障

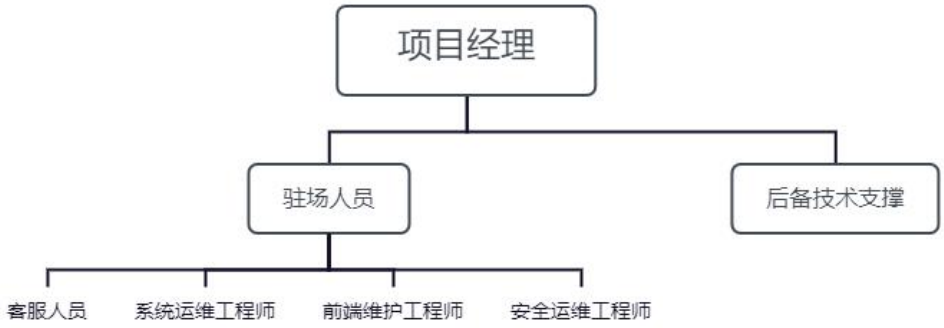

图 3-13 项目组织架构图

运维团队管理主要负责与用户进行沟通、与用户保持亲密联系，了解应用系统情况；负责人员的日常工作，合理的安排人员；制定工作制度，有效的提高工作效率和工作质量；协调各维保单位，建立良好的合作关系；定期向采购单位进行阶段性成果汇报。运维团队成员包括项目经理、运维工程师、客服人员、后备技术支撑等。

提供相对固定的项目服务团队常驻现场人员全权负责现场维护工作，收集客户反馈意见给开发团队整改及现场指导培训客户使用，常驻现场工程师应符合以下要求：具有 2 年以上政府信息化项目建设及维护经验，有较强的组织、协调、沟通能力。运维单位未经采购人方书面同意，不得更换常驻现场工程师；采购人认为常驻现场工程师工作不得力的（如权限不足、技术不熟、管理不当），有权

要求运维单位予以更换，运维单位不得拒绝，由此造成的损失，由运维单位承担。

2、服务质量管理

（1）质量管理目标

1.从质量角度减少系统整体运维中的风险；

2.使系统运维达到本项目运维的要求，符合实际需求。

（2）质量保障措施

1.建立质量管理体系，完善职责分工及有关质量监督制度，落实质量控制责任；

2.建立与质量管理工作相符合的组织机构，由项目管理办公室负责，围绕质量这一中心工作展开全面的质量管理工作；

3.在组织内部做好分工，建立相应的责任制，明确每个岗位及责任。

4.计划时期，协助运维服务机构开展优化运维体系质量保证体系；

5.运维阶段，认真审核运维服务清单，严格按照程序认真进行服务验收；

6.验收阶段，认真审核运维服务文档，严格按照程序进行年度验收。

7.严格执行质检和验收，不符合国家规范、招标投标文件及合同规定质量要求的拒付工程款；

8.在质量达不到要求时充分运用索赔手段。

9.将控制质量与合同管理工作结合起来，对合同条件中的有关质量条款进行集中整理，做科学的分析，为质量控制提供合同依据；

10.利用合同的约束力，调控和调整关系，保障质量工作；

11.利用合同的全面履行和实际履行的原则，保障运维质量。

（3）质量管理体系

贯彻执行质量管理体系的规定，抓好现场管理的每一个环节。

3、服务管理流程

（1）项目启动管理

运维服务项目启动阶段，是重要的里程碑，需要进行质量管理检查，确保项目工作有一个良好的开始。

项目启动阶段，质量检查点如下：

1.质量经理、质量专员是否介入，并了解项目信息。

2.根据运维服务的需要，是否制定了项目的运维服务目录。

3.在项目启动时，是否与成都市城市管理数字化监督管理中心共同进行了项目启动会议，明确了项目的目标、服务内容，服务时间及主要人员，并形成会议纪要。在项目启动阶段，根据配置管理要求，是否建立了项目的配置库。

（2）项目计划管理

项目计划阶段，主要是针对项目规划工作的质量进行检查。

项目计划阶段，质量检查点如下：

1.在维护计划中是否明确了运维服务的主要工作，人力资源投入，考核要求，服务报告提交的形式及频率等。

2.质量专员是否与运维人员共同制定项目质量保证计划。

结合项目实际需要，是否形成了项目的工作流程，如：事件、问题、变更、发布等流程。

（3）项目实施管理

项目实施阶段，是整个运维服务项目，时间最长的阶段，也是最重要的阶段，要进行检查，确保项目实施的质量。

项目实施阶段，质量检查点如下：

1.根据运维服务项目计划是否在进行实施，实施过程中是否得到有效的记录。

2.根据运维服务项目计划的要求，是否定期提交了服务报告（周报、月报、年度维护服务总结等）。

3.根据项目信息安全的要求，是否进行了信息安全培训和检查工作。

4.对事件、问题、变更、配置、发布等工作，是否进行了有效的管理。

5.根据项目规划的培训计划是否进行相应的培训。

（4）项目监控管理

项目监控，是为了确保项目工作得到有效落实，同时需要检查项目监控的工作是否得到落实。

项目监控阶段，质量检查点如下：

1.项目经理针对运维服务项目计划中的要求，是否检查各项工作的完成和质量，确保计划的落实，并有相应的文档记录。

2.项目经理是否定期召开项目例会，检查各项工作的完成情况，针对实施中的困难和问题，进行协调解决。

3.项目中发现的问题，是否得到了记录、跟踪、解决，直到关闭。

4.是否组织了项目客户的回访活动，了解客户对项目的满意度。

（5）项目收尾管理

项目收尾阶段，是项目结束时的重要阶段，为确保项目最终成败，需要进行项目收尾工作的检查。

项目收尾阶段，质量检查点如下：

1.召开项目总结会议，是否与项目干系人共同确认了项目目标的达成。

2.对项目客户进行年度客户满意度调查，客户对整个项目的满意程度是否达标。

3.对项目成员进行考核，确保项目成员的绩效得到客观体现。

4.形成项目文档清单，提交给用户方管理，纳入到过程资产库。

4、运维服务流程

（1）驻场服务流程

系统使用人员在发现系统异常时，及时与驻场服务工程师联系，驻场服务工程师将在第一时间进行故障响应，结合后方技术专家为用户方提供必要的技术支持，确定问题所在并解决问题，问题处理完毕后及时告知使用用户，并将问题处理情况进行归档。

（2）定期巡检服务流程

驻场服务人员在巡检时若发现系统存在异常，及时对出现的问题进行定位，若可直接排除的则立即排除，若不能排除的请求服务团队协助进行问题解决，问题处理完毕后及时告知使用用户，形成巡检记录并将问题处理情况进行归档。

（3）远程支持服务流程

系统使用人员在发现系统异常时，可直接电话、邮件、QQ 群、微信等方式告知驻场服务人员，驻场服务人员将在第一时间为用户方提供必要的技术支持，确定问题所在并解决问题，如果需要现场支持，将安排服务工程师提供现场服务。

5、应急响应保障

制定详尽的应急处理预案，整个流程严谨而有序。在服务维护过程中，意外情况将难以完全避免，针对项目实施的突发风险进行详细分析，并且针对各类突发事件，设计相应的预防与解决措施，同时提供完整的应急处理流程。

（1）应急预案

建立完善的应急预案机制，设置预案事务流程，模拟可能发生的应急事件，确保应急事件发生后可快速的应对。

1.预案事务流程

应急预案的设计应当包括相关部门的协调、应急资源的保证、应急预案启动条件等。

2.相关部门的协调

网络系统的应急预案设计是从保护整体利益，降低网络整体风险为基本出发点，因此，对关键业务的应急保护涉及组织的各个部门和各个方面的配合和支持。关于关键业务应急保护相关部门的关联方式是组织应急预案设计的关键。

3.应急资源的保证

应急预案设计应当将应急活动程序化，并通过程序化确定执行应急预案所许的组织资源，包括人员、设备、资金和其他物资，尤其是人员的保证和其他资源的同意指挥调度等。应急资源的保证还包括运维单位、开发商、系统集成商，以及其它外协和相关单位支持。

4.应急预案的启动条件

组织应急预案的启动条件是组织应急预案设计的重要内容，也是实施应急预案的必要条件。组织应当严格规定应急措施的实施和应急资源调用的程序、决策者和责任人。同时，启动应急预案的决策信息必须来自组织规范的报告制度，并有记录及可追溯。

5.应急预案的演练

组织的应急预案正式批准之前都必须进行演练。演练也可以在仿真条件下进行，但参加演练的人员必须与实际执行应急预案的人员的组成相近。应急预案演练是组织应急预案完善的重要工作，包括应急预案演练的计划安排、演练过程和效果的详细记录，演练活动的评估报告和应急预案改进建议等。

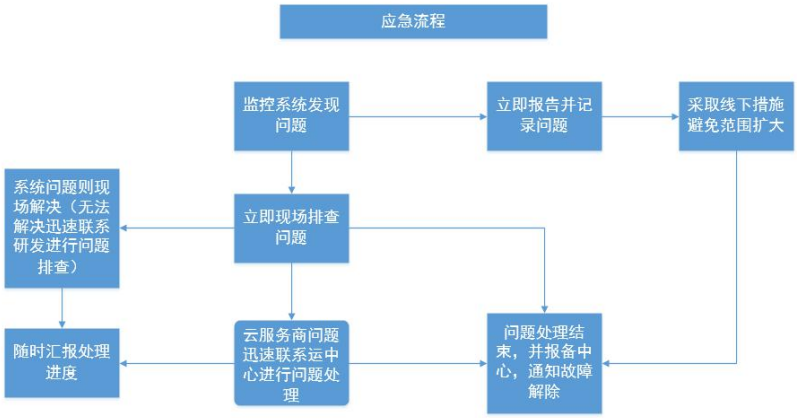

图 3.8 应急响应流程

（2）通讯保障

相关运维人员，保持每天24小时处于开机状态。

（3）人员保障

建立应急协调人机制，驻场工程师必须在发生质量事故后 2 小时内，向项目经理客观反馈问题，由项目经理初步判定项目事故等级，并协调相关人员进行故障处理。

1. 事故分级

按照突发事故严重性和紧急程度对事故进行分级，突发质量事故分为特别重大质量事故、严重质量事故、一般质量事故和轻微质量事故四级。

1)重大：由于不规范操作、不规范管理，对系统生产环境造成严重的数据丢失、系统崩溃、当机，以及造成重大经济损失，严重影响系统使用的质量事故，定义为重大质量事故。

2)严重：由于不规范的情况下对系统生产环境所做操作，而造成对系统生产环境的严重影响（如造成数据丢失、数据混乱）、造成一定程度经济损失，但能通过应急措施补救、挽回部分损失的事故，定义为严重质量事故。

3)一般：由于项目组在未得到客户方授权的情况下对系统生产环境所做操作，而造成对系统生产环境数据损坏或混乱，但未造成较大程度经济损失，通过应急措施可以有效保证数据完备的事故，定义为一般质量事故。

4)轻微：未对系统生产环境造成数据影响，但不符合规范化操作和管理要求，对系统整理质量存在较大风险，且造成项目资产的不完整，造成轻微经济损失的。如未对代码做及时定期的备份，导致代码版本的不完整或代码版本管理混乱的，

定义为轻微质量事故。

2.响应时间

各级故障事件的最晚响应时间为：

表 3.9 响应时间表

确认时间	重大故障事件	严重故障事件	一般故障事件	轻微故障事件
1 小时	技术服务人员			
4 小时	专业工程师	技术服务人员		
24 小时	技术支持专家	技术支持专家	技术服务人员	
48 小时	服务项目经理	服务项目经理	专业工程师	技术服务人员

（4）技术保障

技术专家作为实施专家团队，负责应急处理支持，由项目经理在接到事故时，进行协调通报。

级别在严重（包含）以上的事故，实施专家团队必须指定专人参与事故应急处理，负责支持进行项目影响评估、损失弥补方案等工作。

（七）安全保障

1、日常运维安全

（1）账号口令管理

按照“谁主管，谁负责”原则，系统责任部门负责按照本办法管理单位内部人员及第三方协维人员在系统应用层的账号。

各层账号管理由综合处对账号审批及授权管理，推动制定账号审批流程、表格模版等并落实责任人，监督落实账号申请表、用户账号登记表的维护管理。

各层账号管理由综合处账号审批、创建及删除、权限管理以及口令管理要求执行情况审核机制，接受定期审核。

用户需按照账号审批流程向各责任单位申请所需账号、修改权限或者撤销账号。在账号审批成功并创建后，应对账号口令进行定期修改。并应做到严格保护账号口令，不得故意泄露，否则需承担由此导致安全问题的责任。

（2）终端安全运维管理

终端安全策略配置项应满足以下要求：

1. 系统标准化管理，统一使用正版软件，禁止安装盗版。

2. 密码策略，按照单位内部账号管理办法设置复杂度策略。

3. 配置账户锁定策略，要求设置锁定次数为 5 次以下。

4. 禁用匿名访问网络。

（3）业务安全管理

加强业务内容安全监控，加强对业务内容源引入、内容提供/发布、内容传播等环节的审核和监控，并建立和完善内容安全事件的应急处理机制，确保业务内容提供的健康、合法。

增强业务系统外部接口安全防护，高度重视与外部系统有交互接口的业务平台的安全风险，确保交互协议设计的安全可靠。加强对外部交互协议与接口的拨测，及时发现存在的安全问题。在业务系统建设过程中应在业务系统与外部平台之间规划部署防火墙、流量监控等安全管控措施。

完善业务使用流程和制度，加强对业务各环节流程的审核和监控，及时发现安全问题。对业务要提供准确的核实和确认机制，对业务认证要重点关注敏感认证数据加密、认证算法强度和认证失败次数控制等。

业务平台运维从系统、人员、第三方管理等方面，加强业务平台的运维安全管控，防止业务运维中出现安全隐患。增强业务系统自身的访问控制，严格限制运维人员的账号、权限，确保权限、角色相符合；加强对运维人员的安全意识和技能培训，提高安全运维能力。

2、安全管理

参照《网络安全等级保护安全设计技术要求》（GB/T 25070-2019）中规定的等保三级要求为标准，对信息系统的安全管理体系进行设计。信息安全技术、信息安全产品是信息安全管理的基础，信息安全管理是信息安全的关键，人员管理是信息安全管理的核心，信息安全政策是进行信息安全管理的指导原则，信息安全管理体系是实现信息安全管理最为有效的手段。

（1）安全管理体系

1. 安全管理机构设计

在组织架构方面，应依成都市城市管理数字化监督管理中心现有的组织体系，赋予各层面的组织和个人以安全职责，使原有的组织架构具有信息安全的管理职

能，形成以决策层、管理层和执行层三层组织结构的机构。建立相应岗位设置、安全职责、安全目标。组织架构的建立和充分发挥职能是整个系统安全的前提和基础。

决策层：决策层是最高领导层，负责重大项目事件的决策。小组成员可以包括：成都市城市管理数字化监督管理中心相关领导、负责信息安全工作的总负责人等等。

管理层：管理层直接接受决策层的领导指挥，是系统的管理处室，负责项目各环节的具体领导工作。小组成员可以包括：处室的负责人、各个处室的安全负责人等。

执行层：执行层直接接受管理层的领导指挥，负责各个环节的具体执行实施。小组成员包括：信息处成员、各处室的安全成员等。

2.人员职责设计

决策层：决策层是信息安全管理的最高决策机构，并承担以下责任：

1）审议和批准信息安全保障体系建设规划、信息安全策略、规章制度和信息安全工程建设方案等；

2）为信息安全保障体系建设提供各类必要的资源；

3）对信息安全的宏观问题进行决策；

4）审定信息安全重大突发事件应急预案。

管理层：管理层是信息安全工作的具体组织管理机构。管理机构应承担的职责主要包括：

1）信息安全保障体系建设规划、安全策略、规章制度的制订并组织贯彻落实；

2）规章制度执行情况的监督与检查；

3）信息安全建设项目的组织实施；

4）人员安全，安全教育与培训的实施；

5）协调信息安全日常工作中的各项事宜等。

执行层：执行层是信息安全工作的具体执行机构。负责具体的与信息安全有关的各项实际工作。具体承担的职责主要包括：

1）执行机构的主要职责是管理维护信息安全设备；

2）监测信息安全状态，进行安全审计；

3）在发生安全事件后及时组织有关技术人员进行事件响应。

3.管理制度及规范

信息安全管理制度主要参照公安部等级保护基本要求针对信息系统的管理要求，制定包括规划层、执行层、记录层三个层面的安全管理制度。

规划层：《安全手册》；

执行层：《安全安全建设制度》；《密码管理制度》；《数据备份管理制度》；《日常操作管理制度》；《信息安全风险评估制度》；《外包运维安全管理制度》；《应急响应管理制度》；

记录层：《系统备份记录》；《日常故障维护记录》；《信息安全事件过程记录》；《风险评估记录》。

（2）安全运维体系

本项目设备均部署在成都市电子政务云计算中心机房，所需硬件资源由云中心机房提供。云中心为本项目提供防火墙、数据库审计、日志审计、态势感知、云 waf 服务。由于本次项目所使用的云中心环境已经具备对网络防火墙、入侵检测、病毒防护等相关安全保障手段，所以在本期建设方案中，系统应纳入云计算中心的安全防护体系中。

1.物理环境安全

本期项目系统运行物理环境由云中心提供，云中心物理机房按照 A 级机房要求进行建设，符合本期项目建设要求。

2.网络安全

本项目将部署到政务云三级等保区，由电子政务云为其划分并提供单独的 VLAN 区域，用于部署平台服务端相关系统。

本期项目网络安全由政务云计算中心提供。在安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等网络安全方面，成都市电子政务云已按照等级保护三级标准技术要求建设，部署了相关网络安全系统和设备，并配置了相关的安全策略，满足安全审计、边界完整性检查、入侵防范、恶意代码防范及网络设备防护等相关技术要求。

1）防火墙

网络边界部署防火墙设备，启用访问控制功能；根据数据流设置访问控制策

略，控制粒度为端口级；在会话结束后终止网络连接；启用流量控制功能，限制网络最大流量数及网络连接数。对边界防火墙进行更换，并将用防火墙作为备机。即解决了系统存在的高风险，也解决了防火墙设备冗余备份的问题。

2）IDS、IPS 防护

修改网络设备出厂时的默认口令，且修改后的口令应满足长度大于等于 8 位、含字母数字和字符的强度要求，其它不满足此口令强度要求的，均需要进行修改。IDS 验收后，需及时修改口令；开启日志审计功能。

3）开启 Web 应用防护系统

针对系统中存在 WEB 应用的实际情况，通过应用服务区边界部署 WEB 应用防火墙，提供对应用系统的安全防护，实时过滤和监测 SQL 攻击、跨站脚本攻击等网络攻击事件。主要功能有：WEB 通用攻击防护、协议规范性检查、抗 WEB 扫描器扫描、信息泄漏防护、CC 攻击防护、防护盗链、应用程序错误跟踪、WEB 应用加速、WEB 负载均衡、站点访问审计等。

对 IDS 管理服务器地址和登录设置访问控制。在交换机和防火墙上配置访问控制策略，限制仅管理员用户可进行管理和登录。

4）数据链路防护

采用密码技术保证通信过程中数据的完整性，提供加密的通信隧道，保证传输数据的完整性。利用加密技术对用户单位与系统之间通信的会话过程进行加密传输，保证数据以密文形式传输。

3.主机安全

服务器主机安全由政务云现有的等级保护三级体系主机安全相关措施提供防护。

1）防病毒

应在每台服务器上部署网络版杀毒软件，在所属的服务器上安装防病毒客户端，通过该系统，可实现防病毒的统一管理，统一管理表现为由中心统一发送查杀病毒命令、下达版本升级提示，并及时掌握系统中心的病毒分布情况等，具体要求如下：

支持系统加固、应用程序控制、木马行为防御木马入侵拦截（网站拦截）、木马入侵拦截（U 盘拦截）、智能防御自定义白名单、自我保护等主动防御策略

下发。

支持远程对防病毒客户端进行漏洞扫描，并能进行补丁的自动分发。

支持多种病毒报警方式,包括发送到管理控制台、声音报警、发送邮件(SMTP)、发送 SNMP 陷阱(SNMP Trap)、显示消息框(Message)、保存 NT 事件日志(NT Log)、报告给上级中心、支持 SysLog 日志报警，同时，用户可自订制报警方式。

具有病毒日志查询与统计,可以随时对网络中病毒发生的情况进行查询统计,能按时间（日、周或任意时间段)、按 IP 地址、机器名、按病毒名称、病毒类型进行统计查询。

2）系统安全加固

针对业务平台操作系统存在的安全漏洞，采取人工修改配置参数等措施。本项目中系统环境由云中心负责提供，因此对项目所涉及到 windows server2008/2012 安全加固不再另行考虑，由云中心实现系统级加固策略。

4.应用安全

1）数据加密

交换双方的数据支持加密通信,支持从端到服务器之间机密信息的高强度加密传输（如 SM 系列加密等)。

2）身份鉴别

在应用服务区前部署身份认证网关，为登录用户颁发数据证书，作为其全网唯一的身份标识。按照等级保护要求，设置相应的安全策略，包括用户口令具有良好复杂度并定期更换，启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

3）访问控制

在各应用系统设计时，设计相应的用户权限管理模块，根据用户不同的角色设置相应的访问权限，为不同账户授予其承担任务所需的最小权限，防止用户的越权访问。

系统对用户登陆过程进行记录，连续登陆失败多次后，可暂时锁定用户。

对用户在线空闲操作的时间限制，强制用户重新登录。

4）系统日志

建立严格的日志记录机制，记录系统启动与关闭情况和系统工作情况。提供

管理员操作日志、用户登录日志和用户操作日志，确保日志能满足对人员操作进行事后审计。

5）安全审计

在各应用系统设计时，必须设计相应的安全审计模块，实现对用户访问应用系统各种操作行为的安全审计，生成审计日志。

6）软件容错

各应用系统须具有软件容错机制，通过进行代码审核，对输入数据进行检查，保证符合规定，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

5.运行安全管理策略

运维阶段是整个平台生命周期中最长的一个阶段，也是安全问题最集中的阶段，因此该阶段的安全管理对整个平台的安全应起到非常关键的作用。在这个阶段的建设中，不仅将依据规范从风险评估、安全审计、日常维护、信息资产、口令、电子文档、系统应急等方面对运维过程中的重要管理问题进行安全管理建设，还应进行全方位的、系统的运维保障管理和技术体系的应用。

安全运维管理是对安全管理体系建设各项制度进行细化、落实，将制定可操作的体系化的规范和流程，与安全管理体系和技术体系一起形成层次化的安全策略体系。

运维体系的有效运行远不是安全设备运行那样简单，系统安全运维体系将以安全外包、安全培训为基础，依托安全设备，以系统和网络实现真正的风险管理为目标，根据实际环境和需求进行运维工作的组合及运维形式的调整，最终提供定期、不定期、实时等形式的运维管理。通过各种表现形式的安全运维，在系统内部建立 PDCA 循环机制，实现对信息系统的整体安全运维保障。

系统安全运维体系建设将针对各子系统自身的业务特点，开展信息安全运维工作，达到与现有的业务管理体系及安全技术、管理体系相互依托、高度融合，安全管理体系将融入到日常的运维体系当中，也争取将信息安全指标纳入到正常的绩效考核体系中，从组织、人员、运维等方进行体现管理本质的信息安全运维体系建设，目标是实现系统的稳定运营。

安全运维体系的高效运作不仅仅是通过管理手段实现，而应以安全服务、安

全技术手段作为支持，技术监控行为要与安全管理行为相结合。

应通过下发文件、会议宣贯、组织学习、专业培训等多种方式对制定的安全规划、管理体系、运维体系等进行宣贯，确保所有相关人员熟悉、理解和遵守相关的流程和规范。

应定期审查流程和规范的执行情况，考核信息安全运维人员完成安全运维工作的规范程度。

（八）成果交付专栏（以下材料作为阶段验收必备材料和付款依据）

1、半月、月、季度、年度运维报告（主要含系统运行、日常巡检、故障记录、驻场人员情况等）；

2、专项运维整改报告包括但不限于：三级等保整改情况报告、攻防演练总结报告、重特大事故情况处理报告、系统漏洞整改情况报告等。

注：以上带“★”为实质性要求，不满足的将做无效响应。

三、商务条款（实质性要求）

（一）最高限价要求

本项目最高限价为：人民币 98.7 万元，供应商报价高于此限价的，其响应文件按无效处理。

（二）服务期限要求

本项目服务期为一年（12 个月）

（三）服务地点要求

本项目服务常驻地点为成都市城市管理数字化监督管理中心（成都市青羊区科联街 3 号），同时根据服务范围及内容要求，按需到采购人指定地点开展运维服务。

（四）付款方式要求

成交供应商在合同签订后15个工作日内向采购人提供详细的维护服务实施方案、目标任务书和技术保障方案等，并经采购人审核通过后开展系统运维相关服务；服务款每季度结算一次，在季度服务质量考核通过后，按服务总金额25%的标准在扣减考核罚金后进行支付（最后一季度尾款，在项目服务期满且通过采购人组织的履约验收后予以支付）。

（五）项目资料要求

维护团队定期提供服务报告，服务期结束前应提供服务年报，并对每一次重大故障和问题的原因、解决方法、完成情况等形成专门报告，及时报送用户部门和服务管理部门。在运维服务过程中将产生不限于以下的记录和报告；按年、季度、月制作资源体系运行分析报告，全方位和多角度地呈现运行状况，发现问题，总结经验，为资源体系管理工作的针对性改善和效能提升提供客观基础，包括但不限于：系统运行报告、日常巡检报告、故障记录报告等。

（六）服务质量要求

供应商提供的服务质量须符合国家信息技术运行维护相关标准，服务期内所提供的所有替代备品和更换备件应满足国家和行业相关技术标准。

（七）违约责任

1. 如因供应商原因要求提前解除本合同的，须按本合同总金额的 25%向采购人承担违约责任，违约金不足以弥补采购人损失的，采购人有权要求供应商进行补足。

2. 供应商季度考核得分低于 60 分，视为运维服务不合格。供应商须按本合同总金额的 25%向采购人承担违约责任，采购人有权扣除第四季度服务费作为违约金，

同时，违约金不足以弥补采购人损失的，采购人有权要求供应商进行补足。

3.如因供应商工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任。

4.合同签订后15个工作日内，供应商如不能提供完全符合本项目要求的服务人员和服务方案，采购人将终止合同执行，并保留进一步追究供应商相关责任的权利，同时将供应商履约情况上报成都市财政局。

5.服务期内，供应商在书面告知的情况下对服务人员进行变更/调整未获采购人同意或供应商在未书面告知采购人的情况下，擅自对服务团队人员进行变更/调整，供应商须承担2000.00元/人/次的违约金，并在采购人规定的时限内，恢复原有岗位人员配备，逾期未恢复的，每延期1天（不足1天按1天计算）增加违约金1000.00元/人/次。

6.服务期内，供应商在书面告知并获采购人同意的情况下对项目驻场服务人员变更超过1人/次（不含），须承担2,000.00元/人/次的违约金。

7.当服务范围内的系统发生故障后，供应商应在规定的时限内予以处置和恢复，若供应商无故未予以恢复，除在季度履约质量考核扣分之外，每延期1小时（不足1小时按1小时计算）扣除季度服务总额的千分之五，单次故障扣款累计不超过季度服务总额的百分之八。

8.在服务期内，扣款累计达到服务总额的百分之十五或供应商因服务保障不力对采购人工作造成了重大负面影响（重大负面影响包括但不限于：因系统故障，致使采购人连续24小时以上不能正常工作；或其他经采购人认定为重大负面影响的），采购人有权单方面终止服务，并保留进一步追究供应商相关责任的权利，同时将供应商履约情况上报成都市财政局。

9.供应商有其他任何违约行为，在季度履约质量考核扣分之外，应在采购人指出后予以整改，未在采购人指定的期限内予以整改的，每延期1天（不足1天按1天计算）供应商应承担单项违约1000元/天的违约金。

10.供应商应**书面承诺**，所承担的违约金，采购人可直接从应支付给供应商的服务款项中扣除。

11.供应商支付违约金并不能免除按服务规定供应商所应承担的义务。

12.供应商应**书面承诺**，所未能按约履行维护义务的，采购人有权选择第三方承

担维护工作，供应商应承担的违约金不足以支付所产生的费用的部分由供应商承担，供应商不得提出异议。

（八）服务质量考核

1、考核程序及程序

采用季度考核、按季度结算的方式进行，具体考核程序如下：

（1）维护服务合同开始后每季度末，供应商对该季度运维服务情况进行自查，形成季度总结报告，在下一季度开始后 5 个工作日内报采购人。

（2）采购人根据季度总结报告和相关运维资料，结合自身对供应商服务工作的掌握情况，依据运维服务考核标准得出其该季度的考核分数，季度考核得分作为季度维护费用结算的依据。

（3）采购人根据当年各季度考核得分的平均分作为年度考核结果。

2、考核结果应用

（1）运维服务合同中应将评价结果与支付条款相挂钩，加分总数不大于扣分总数；

（2）服务评价结果是衡量运维服务运维单位服务能力的重要依据，以往的服务评价结果应作为选择运维服务运维单位的重要参考；

（3）每扣1分对应扣除当季服务费100元服务费，每季度服务费为总费用四分之一；

（4）履约验收应在第四阶段考核完成后进行；

（5）供应商季度考核得分还作为年度考核得分的依据，年度考核得分为各季度考核得分的算数平均数。如供应商季度考核得分低于60分，视为运维服务不合格，采购人有权提前解除合同，并保留进一步追究供应商相关责任的权利，同时将供应商履约情况上报成都市财政局。

3、考核内容

序号	考核项目	考核子项	考核标准
1	履约能力	按照磋商及响应文件及合同要求完成服务采购期内建设内容	按未完成内容比扣分

序号	考核项目	考核子项	考核标准
2	驻场保障服务	日常维护	按照巡检表的要求定期向采购单位提交书面巡检报告。未按照要求进行巡检、检测和记录，扣 2 分；检测项目缺失每项扣 1 分。
		驻场服务	是否按照问题处理流程，及时对用户反馈问题进行受理、交办、反馈、结案。未及时回应的，以半小时为阶段，每半小时扣一分，无上限。
	专项支撑服务	故障应急	一级故障出现时未按时响应扣 3 分，未按规定时间处理完成扣 3 分，未及时提交故障报告扣 1 分； 二级故障出现时未按时响应扣 2 分，未按规定时间处理完成扣 2 分，未及时提交故障报告扣 1 分； 三级故障出现时未按时响应扣 1 分，未按规定时间处理完成扣 1 分，未及时提交故障报告扣 1 分； 四级故障出现时未按时响应、未按规定时间处理扣 1 分，未及时提交故障报告扣 1 分； 故障处理记录、故障报告缺失或未达到用户要求的，每有一次扣 1 分，可累计，扣完为止。
		重点保障值守工作	根据制定的服务保障方案实施保障，未提供保障服务的，每有一次扣 1 分；未达到用户要求的，每有一项/次扣 0.5 分

序号	考核项目	考核子项	考核标准
			保障过程中，出现一般性失误或造成不良影响的，每有一次扣 0.5 分； 出现重大失误或造成恶劣影响的，每有一次扣 2 分； 出现特别重大失误或造成非常恶劣，每有一次扣 5 分
3	信息安全服务	服务期间，应尽量避免系统出现安全问题；系统出现安全问题后应及时按照预设流程或应急方案进行处置，做好记录；事后应进行专题分析，提交专题报告，并优化系统	特别重大安全事故发生未按时响应或未按规定流程处置的，每发生一次扣 5 分； 重大安全事故发生时未按时响应或未按规定流程处置的，每发生一次扣 4 分； 较大安全事故发生时未按时响应或未按规定流程处置的每有 1 次扣 2 分； 一般安全事故发生时未按时响应或未按规定流程处置的每有 1 次扣 0.5 分； 安全事故后续分析中，如认定运维单位对特别重大安全事故发生负有直接责任的，每次扣 10 分；对重大安全事故发生负有直接责任的，每次扣 8 分；对较大安全事故发生负有直接责任的，每次扣 5 分；对一般安全事故发生负有直接责任的，每次扣 5 分 系统出现安全问题后，未进行有效专题分析、未提交专题分析报告或未进行有效优化措施的，每有一项/次，扣 0.5 分；

序号	考核项目	考核子项	考核标准
			可累计，扣完为止。
4	系统稳定性	服务期间，各应用系统运行稳定，故障少	对于运维单位负有责任的系统故障，累计时间大于 30 分钟且小于等于 1 小时，扣 1 分；考核周期累计时间大于 5 分钟且小于等于 15 分钟，每有一次扣 0.5 分
			对于运维单位负有责任的系统故障，考核周期系统累计故障时间大于 1 小时，每有一次扣 0.5 分
5	服务团队	根据采购单位要求，运维单位应提供相应数量的驻场服务团队	系统在重大活动或会议期间出现故障并造成不良影响的，每有一次扣 0.5 分；后果特别恶劣的扣 1 分
		运维服务单位应进行岗位设计，制定岗位职责。	无岗位设计和岗位职责扣 2 分；缺失每项扣 0.5 分。
		运维技术人员应具备信息技术基础知识、运维岗位所需的专业知识及信息系统所支撑业务的相关业务知识。	未配置相应业务知识人员，扣 1 分。
		驻场人员稳定性	每季度驻场人员不超过 2 人次（含 2 人次）。每超过 1 人次扣 1 分。
6	服务方案	本期服务开始前 15 日，制定年度服务计划和服务方案，并按季度来更新。	未制定年度服务计划或服务方案，每有一次扣 2 分； 未按时提交合格的服务计划方案，延期 1 天扣 0.1 分； 可累计，扣完为止。
7		按照采购单位和项目实	未制定服务保障方案，每有一次扣 2

序号	考核项目	考核子项	考核标准
		际需求，制定服务保障方案，包含日常服务保障方案、应急保障方案、重大活动保障方案。	分； 未按时提交合格的服务保障方案，延期 1 天扣 0.1 分； 可累计，扣完为止。
8		按照甲方要求按时提交日巡检记录，月度、季度、年度服务报告，不定期按照用户需求提交数据分析报告。	未提供日巡检记录，每有一次扣 0.2 分； 未提供月度服务报告，每有一次扣 0.5 分； 未提供季度服务报告，每有一次扣 0.5 分； 未提供年度服务报告，每有一次扣 1 分； 未提供数据分析报告，每有一次扣 0.5 分； 未按时提交合格的服务报告和数据分析报告，每延期 1 天扣 0.1 分； 可累计，扣完为止。
9	用户满意度	对服务使用方每季度至少进行一次用户满意度调查	各使用方各季度满意度调查的平均值低于 90%，每低 1%扣 0.3 分。
		用户投诉	运维团队和人员在开展工作时需保持良好的态度，提供专业和耐心的技术支持服务。受到各级用户书面投诉的，每次扣 2 分。受到用户书面表扬的每次加 2 分。
10	超时工作	加班	应采购人要求加班完成工作，每次加 0.5 分，1 小时后每加班 1 小时加 0.1

序号	考核项目	考核子项	考核标准
			分。
11	建设性意见	对用户单位信息化建设提出建设性意见	对用户单位信息化工作提出建设性意见，每被采纳一项加 0.5 分，同时配合完成相应文档编写工作，每份文档加 1 分
12	重大保障完成情况	完成重大保障任务	依采购单位和实际需求而需要完成的重大保障任务，运维单位保障工作完成出色，可酌情加 1-10 分。