市政务云创新区域政务移动端服务（2025-2026年）项目采购需求

# 项目概述

项目背景：拟通过统筹集约购买市政务云PaaS服务的方式，采购一年周期的市政务云创新区域政务移动端服务（目前为“随申办政务云”），有力支撑全市公务人员即时通讯和政务一体化办公等工作安全、稳定、便捷和高效地开展，数字赋能一网通办、一网统管、值班值守、防汛防台、应急指挥和行业监管等重点工作。不断完善创新区域政务移动端PaaS服务的长效运营机制，持续提升市级政务云综合服务支撑能力。项目要求支持不少30万用户账号开通的能力（据初步估算2026年度用户可能会达到40万），信创化私有化部署，通过相关测试测评，做好服务期内的运营服务、更新迭代和安全保障等工作。本项目属于市政务云PaaS服务，服务类别为平台软件服务，服务子类为政务移动端。

服务期限：自签订合同生效之日起一年

服务地点：上海市静安区

预算金额：10000000元

采购金额（最高限价）：10000000元

采购方式：公开招标

面向企业类型：大中小微

是否接受联合体投标：否

# 服务范围

## 系统重要等级

本项目为市大数据中心重要信息系统

## 维护清单

|  |  |
| --- | --- |
| **序号** | **模块名称** |
| 1 | 创新区域政务移动端 |

## 服务范围

本项目的服务范围为市级政务云使用单位。目标用户为全市各级党委、人大、政府、政协、法院、检察院、人民团体、民主党派、中央驻沪单位等系统以及其他相关单位通过一体化办公平台开展政务办公和业务处理的工作人员。

服务要求全信创本地化部署，通过相关测试测评，做好服务期内的运营服务、更新迭代和安全保障等工作。

# 项目整体要求

## 技术要求

1. 系统部署资源要求：投标人提供的服务应当具备为本项目服务范围提供服务的能力，其中涉及基础资源使用的（包括但不限于计算、存储、备份、网络等）应当使用市级政务云基础设施服务资源，部署方式需要得到采购人的确认。
2. 接口服务要求：投标人应当提供包括但不限于API发布、管理、流量控制、用户管理功能的API网关，投标人提供的能力中涉及API方式提供的应当具备通过API网关服务的能力。各委办局及业务单位自主开发的应用程序接口由一体化办公平台统一对接。要求移动端适配安卓、原生鸿蒙版操作系统，PC客户端适配主流操作系统及国产芯片。
3. 安全隔离要求：投标人提供的服务涉及集中部署的应该符合网络安全等级保护三级的要求并通过安全测评，开展安全加固工作，包括但不限于安全策略配置、安全扫描和系统漏洞的加固，配合使用单位完成应用的等级保护工作。提供软件介质部署在使用单位资源上的，应当提供安全漏洞修复补丁并提供技术支持，配合使用单位完成应用的等级保护工作。
4. 密码服务要求：所提供的服务及提供服务所需的软/硬件设备符合《中华人民共和国密码法》及国家和本市密码管理部门的相关要求。
5. 服务交付要求：投标人提供的市政务云PaaS服务，应当面向使用单位提供每个服务项的服务接入方式，包括但不限于界面、API接口、文件等。
6. 投标人提供的产品和服务应满足国家和本市有关工作秘密信息技术防护的要求，即时通讯应满足承载工作MM文件的能力。
7. 投标人在中标后应当配合采购人完成服务考核评估工作，并负责对已经出现的服务问题进行整改。

## 服务采购要求

1. 服务描述：提供移动平台统一底座和移动端统一入口，汇聚本市各级组织的政务移动端服务，打造面向政务工作人员的一站式工作平台，通过统一应用管理、工作台、集约化管理中心，实现信息内容的整合和集中展现。
2. 服务范围：市委部门、市人大部门、市政府部门、市政协部门、法院系统、检察院系统、人民团体、民主党派、相关中央在沪单位等系统以及其他相关单位通过一体化办公平台开展政务办公和业务处理的工作人员。
3. 投标产品数量及授权要求：投标产品数量1个，用于投标的服务产品非投标方自有的情况下，需要提供原产品厂商授权书（每个产品对应一张授权书）。
4. 人员要求：每个服务产品应当提供不少于1人的专职支持人员。
5. 部署区域：支持在上海市级电子政务云XC云环境进行部署。
6. 部署模式：支持单机和集群部署模式。
7. 功能要求：（需提供原厂承诺并加盖公章）

（1）提供使用单位内部和对外的即时沟通、移动办公、音视频会议、一体化集成化办公能力，加速政府内外部信息高速流转，提升政务协同效率，满足新时代政务工作线上化、移动化协同场景的需要。

（2）平台支持移动APP和PC客户端的终端呈现方式，结合协同开放平台和应用市场实现政务应用的多端统一分发和统一管理，实现用户在多端统一的登录认证和权限控制，保持用户在多端的业务一致性，为用户带来方便、快捷、良好的多端体验。

（3）平台内置即时通讯工具，提供内部即时通讯，实现单位内部的信息发送、文件传输、单点登录、在线感知、水印加密、消息提醒、视频通话，即时发送对话、消息、文件等。支持手机客户端，实现手机APP与PC端平台的无缝集成。可以快速查询历史沟通记录。支持文字、表情、图片和附件的发送。也可支持平台内相关流程、文档、人事等信息的直接关联发送。

（4）针对移动终端、通信网络、移动接入、以及服务端所面临的风险和威胁提供必要的策略和措施，提供安全可信的移动互联网化办公协同能力。包括但不限于：支持禁用成员在客户端“接收”和“拍摄”的图片或视频保存到手机相册；支持禁用聊天记录分享；支持仅在当前app内复制粘贴；支持禁用文件在其他应用打开或保存到手机；支持禁用内置浏览器的复制链接、分享、在外部浏览器打开等；支持禁用通过邮件发送；支持移动端防截屏、防录屏。

（5）敏感词过滤，添加的关键字在聊天消息中被命中后，客户端会提示不可以发送。支持批量导入、手动添加和API接口同步多种方式，保障敏感词的快速更新。支持网址屏蔽，添加网址后，名单内的网址将不可以被访问。

（6）支持控制用户登录网络环境和终端类型，比如特殊岗位在外网环境下不允许PC端登录。支持设备管理，管理员可以远程查询设备的使用情况，可指定设备下线，禁用、远程擦除数据等。

（7）支持采用国密算法加密，实现信息传输全过程的端到端加密，支持分级加密逻辑，针对组织架构采用单位级密钥加密，针对聊天会话根据不同用户采用不同密钥加密，针对每个文件采用不同密钥加密。

（8）单人音视频通话不受并发限制，支持所有用户同时使用互联网终端并发音视频通话。

（9）支持H5形式的应用对接集成，并为H5开放界面交互、导航栏、背景、置顶、自定义组件、下载、上传、数据缓存、媒体、视频、音频、录音、相机、富文本、位置、文件、陀螺仪、扫码、振动等接口。

（10）持设备登录限制，如Android、windows、mac、pad、Linux、Web等。支持按部门、标签、成员等设置白名单，白名单成员不受登录客户端平台策略限制。

（11）移动端信息防泄漏:支持禁用成员在客户端“接收”和“拍摄”的图片或视频保存到手机相册;支持禁用聊天记录分享;支持仅在当前app内复制粘贴;支持禁用文件在其他应用打开或保存到手机:支持禁用内置浏览器的复制链接、分享、在外部浏览器打开等;支持禁用通过邮件发送;支持移动端防截屏、防录屏。

（12）要求服务器端私有化部署到用户的网络环境中，数据存储在用户机房，在与互联网的连接完全断开的情况下(即与互联网物理隔离的环境下)，可以支持纯内部网络环境下的即时通讯、通讯录访问、应用访问等功能。

（13）服务器端支持在搭载国产芯片和国产操作系统的环境中部署：服务器端支持在搭载国产芯片的环境中部署，针对鲲鹏、海光、飞腾环境部署；服务器端支持国产操作系统上进行部署，针对麒麟和统信UOS部署。

1. 性能要求：

（1）具备支持不少于30万用户账号开通的能力。具备支持月平均活跃用户不少于6万的能力。

（2）消息业务响应速度（包含各类文本信息、群聊)≤3s。

（3）系统平均响应时间≤3s。

1. 兼容性要求：

（1）支持工作台集成H5应用。

（2）取得商用密码产品检测认证证书。

1. 安全性要求：

（1）数据安全性要求：依照两副本模式存储，保障数据一致性，防止数据丢失。

（2）提供的软件产品通过第三方等保测评。

1. 服务要求：提供包括不限于该服务的安装使用材料、产品使用介质、版本升级介质、产品API、适配改造、安全问题修复、应急保障、产品文档、培训咨询、巡检服务、性能调优、重要活动和重大节假日现场值守保障等保障服务。
2. 对接要求：提供服务产品对接的API接口，对接内容包括不限于产品使用情况、计量基础数据、运行监控数据、事件告警等内容。
3. 验收考核要求：

（1）满足以上人员要求、部署要求、功能要求、性能要求、兼容性要求、安全性要求、服务要求、管理要求。

（2）提供服务对应软件产品的使用详情，以及提供用户开通授权的使用详情。

（3）服务结算按照已开通的用户并且在服务期内实际使用的用户进行结算，服务期内已开通的用户无登录使用记录的，不在结算范围内。

## 原厂授权要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **投标产品数量上线** | **原厂授权\*** |
| 1 | 创新区域政务移动端 | 1 | 需要 |

1.如为投标人自有产品，需提供承诺函。

2.如非投标人自有产品，需提供原厂授权，每个产品对应一张授权书。

# 软件系统运维需求

在中标后应当对提供的服务内容提供培训服务、运维保障、迭代升级、安全保障等服务。包括但不限于政务云服务的环境搭建、软件安装、运维支持、业务场景接入、服务使用培训等内容，以及按照承诺的服务标准提供各类售后服务和服务的升级维护。

1. 投标人在中标后提供热线电话、电子邮件和在线网站等技术支持方式，提供 7\*24 小时电话响应服务，以及5\*8小时的现场运维服务。重大节点强化保障，确保服务可用性不低于99.99%。
2. 投标人在中标后应当建立健全服务运维安全管理制度，提供服务安全保障和监控预警工作。
3. 系统扩容：投标人应承诺，在日常运维过程中，当服务资源使用率超出限定额度或服务数量、功能、性能等方面不满足最终用户使用要求时，投标人需对现有服务能力进行扩容。在采购人发起扩容需求后，投标方需在1个工作日内响应，在2个工作日内完成扩容申请提交，同时向采购人提交扩容后服务的资源情况报告。
4. 日常监控、巡检：投标人在中标后应当对提供的服务进行日常监控、巡检，包括监控告警的处理，巡检异常的处理等；投标人在中标后需制定维护管理规定，并按照规定中要求维护项目以及制定详细的作业计划并执行。
5. 迁移及升级割接：开展业务系统迁移割接和政务云平台软硬件升级割接；中标人在升级前制定完善的操作实施方案，在方案中尽量降低对上层业务系统的影响；对于可能影响上层业务系统的各类操作，应全面评估操作影响，并提前通知采购人具体操作计划安排，在采购人的相关业务部门同意后方可执行操作。
6. 服务升级：投标人在中标后应当承诺，在日常运维过程中提供的服务功能、性能等方面需要升级更新时，投标人在中标后应当在2工作日内响应，经采购人确认升级方案后，按照计划完成升级任务。
7. 系统中断：由于服务维护等原因需要中断系统进行升级操作时，提前至少72小时（重大自然灾害除外）通知采购人做好相关准备工作，同意后方可实施。
8. 配置实施及管理：进行服务各软硬件设备的基础配置、IP配置、角色用途、账号密码等的统一配置实施及配置管理。
9. 应急处理和响应：投标人在中标后应当建立完善的应急管理体系，管理体系涵盖应急处理的应急等级、响应时效、职责分工和处理界面，每个处理流程留有电子化记录并在每个处理环节中落实到投标人在中标后的部门和相应的处理接口人。按照故障等级不同，需要有不同的处理时长和故障恢复时限。
10. 投标人提供的服务应当包含整体平台涉及的操作系统及相关软件，以及对应的软件安装服务、软件支撑服务、软件开通服务、软件维护服务、业务场景接入服务、软件升级管理以及服务使用培训等服务。
11. 重点工作保障：节假日和重大活动等期间需配合甲方进行平台运行和信息安全的重点保障。
12. 投标人应当提供服务相关的应急演练与应急响应服务，根据采购人的要求提供针对性演练，制订应急预案，每年组织至少2次应急演练。当发生重大应急事件时，需在负责单位牵头下实施应急响应操作，并在事后制定重大事件报告。

## 日常维护业务需求

## 现场值班工作需求

服务提供方需建立有《系统应急预案》等相应管理制度。

现场维护人员工作日5\*8小时的现场值班工作,特殊时期内，根据要求执行值班安排。对值班情况有记录文档。遇到应急突发事件时能按照应急流程制度处理相关问题。

## 应用监控需求

服务提供方需对该系统进行日常应用监控、网页监控、服务器状态监控、应用数据同步工作，以书面或电子方式记录相关监控结果。

对重要的应用服务器能提供实时状态监控手段和发生突发故障时的应急保障支持。

### 客户端维护需求

现场维护人员能够为客户端提供常用软件的安装配置服务，并且为用户提供一系列的系统优化与调整。

针对该系统中所需的特定软件及相关设置，需维护人员都能够给予安装调试服务。

### 电话/工作群支持需求

为系统提供电话/工作群（建在创新区域政务移动端）技术支持，解决业务部门在使用中遇到的相关问题，并跟踪直至问题最终解决。

### 现场技术支持需求

紧急情况下，为用户提供现场技术支持服务。提供7\*24 小时电话响应服务，以及5\*8小时的现场运维服务。

当用户遇到电话支持升级时（即电话支持无法解决），可由维护人员进行现场故障排查，并提供相应技术支持服务。

对部分需要现场安装调试的系统，服务提供方需要在安装前与现场工作人员取得联系，在确认计算机配置、操作系统及网络环境后进行现场安装，并提供技术保障。

## 应用系统优化需求

### 业务需求变更需求

服务提供方需对用户提出的需求变更进行相应处置。

（1）服务提供方的设计和开发人员需要保证原系统设计架构不变的情况下，对系统提供业务需求变更服务。

（2）当业务部门提出需求变更时，能够安排专人负责进行需求分析，听取用户需求并与用户交换意见，提出变更中存在的问题并提供相应的解决方案。

（3）确认需求分析后填报《需求变更设计文档》，进行业务需求变更跟踪流程，直到变更实施完成。

### 新系统设计与实施需求

服务提供方开发人员能够及时发现现有系统中的不足，在不影响现有系统正常运行的情况下不断完善业务功能。

面对重大业务需求，或提供重大活动后方保障工作时，服务提供方能够快速响应，安排相关开发人员进行调研并在第一时间内完成方案设计、系统实施、测试更新以及落实跟踪回访工作。

## 数据库维护需求

服务提供方需有相关保障制度。能提供以下基本的维护内容项目：

（1）对数据库情况进行每周巡检、月度系统巡检工作，在巡检完成后记录下巡检信息。

（2）提供两副本的业务数据服务。

（3）能对与关键应用相关的数据库服务器进行性能优化以及系统优化工作。

（4）当数据库发生故障时按照《应急维护方案》服务提供方相关技术支持人员能够迅速赶到现场处理问题。

## 信息化资产维护需求

服务提供方需依托上海市大数据中心-一体化运营平台对该系统进行常态化的信息化资产梳理工作。包括但不限于：将系统与在用的服务器等资源进行关联；纠正更新系统基本信息；更新系统应急演练、等保备案情况等信息。

# 服务质量考核要求

服务质量由市大数据中心相关部门和五分中心考核。第三方监管团队应大数据中心要求，基于材料审查、实地检查、数据接口、问卷调查等多种方式，定期按考核指标进行考核。

# 验收要求

本项目中应当根据本市和市大数据中心数字化项目验收要求提供相关材料，并指派专人负责验收。采购人在收到投标人提交材料后的20个工作日内组织验收。如属于投标人原因致使未能通过验收的，投标人应当在15个工作日内进行整改，并自行承担相关整改费用，再次接受采购人的验收，直至符合约定要求。采购人有权委托第三方机构进行验收，对此投标人应当配合。如本项目连续3次验收未通过，采购人有权解除项目并追究投标人的违约责任。

服务期限终止前，投标人应当以书面形式向采购人提交验收材料，包括不限于招标文件、投标文件、合同、用户操作手册、项目实施方案及计划、项目运行维护记录、应急预案、项目完成情况确认表、项目过程性材料（会议纪要、用户培训记录、应急演练记录等）、第三方测试测评报告及本项目总结报告等。

# 付款方式

1、预付费：合同签订生效且收到发票后10个工作日内甲方向乙方预付服务费用100万元。该预付费用于抵扣将来实际发生的服务费用。

2、进度服务费1：合同周期过半、通过甲方组织的本项目周期检查且甲方收到乙方开具的等额发票后10个工作日内，支付至合同金额的50%。

3、进度服务费2：通过甲方组织的本项目周期验收且甲方收到乙方开具的等额发票后10个工作日内，支付至合同金额的80%。

4、服务费尾款：最终验收通过后，甲方根据上级主管部门审定的最终合同总价与已支付服务费（即预付费+两次进度服务费）的情况与乙方结算服务费尾款。若已支付服务费＜本项目最终合同总价，甲方在乙方开具等额发票后的10个工作日内支付服务费尾款。若已支付服务费≥本项目最终合同总价，则按财政管理规定做好后续结算处理。乙方在此同意接受上级主管部门审定的最终合同总价。

5、本项目最终实际结算价格不超过项目预算人民币1000万元。

# 报价一览表

项目名称：市政务云创新区域政务移动端服务（2025-2026年）

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **服务类别** | **服务子类** | **服务项** | **服务子项** | **单位** | **创新服务** | | |
| **单价限价（元/年）** | **单位报价（元/年）** | **年封顶价\*（元）** |
| 1 | 平台软件服务 | 政务移动端 | 创新区域政务移动端 | 0-2万用户 | 个 | 260.00 |  | 10,000,000.00 |
| 2-10万用户 | 个 | 160.00 |  |
| >10万用户 | 个 | 125.00 |  |

投标人名称:

(盖章)

法定代表人或授权代表(签字):

日期:

说明:

1. ★本项目设置服务单价限价，服务单价不应超出报价表中每项服务单价最高限价。
2. 本项目依照6万个活跃用户作为基准计算投标总价，投标报价总价不得高于最高限价。
3. 初步估算的市级部门和单位用户为10万，初步估算的市级部门和单位月活跃用户约6万。主要包括市级党委、人大、政府、政协、法院、检察院、人民团体、民主党派、长三角示范区（含示范区执委会、青浦区、吴江区、嘉善区相关用户）部分中央驻沪单位等系统以及其他相关单位的公务人员，应急直播、值班值守、防汛视频调度、防灾减灾、进博保障、统一综合执法、督查码应用、专项行动等相关应用的公务人员。届时以实际使用的部门、单位和用户数为准。
4. 各区创新区域政务移动端服务的费用结算，根据本区的实际使用数量，参照《关于在市政务云领域试行统采分签制度的意见》[沪府办字〔2022〕10号]执行。
5. 所有价格均系用人民币表示，单位为元，精确到分。
6. 投标人应按照《招标需求》和《投标人须知》的要求报价。
7. 阶梯价格计算公式：

总费用 = 第一阶梯活跃用户数×第一阶梯单价+第二阶梯活跃用户数×第二阶梯单价+第三阶梯活跃用户数×第三阶梯单价。

其中，各个阶梯活跃用户数的计算方法为：

第一阶梯活跃用户数 = min（总活跃用户数，20000）；总活跃用户数∈（0,20000]

第二阶梯活跃用户数 = min( max(0，总活跃用户数 - 20,000)，80000)；总活跃用户数∈（20000,100000]

第三阶梯活跃用户数 = max（0，总活跃用户数-100000）；总活跃用户数∈（100000,+∞）

# 服务组织和人员要求

投标人应当为本项目单独建立管理组织，配置相应运营团队。

驻场支持：投标人须为本项目提供不少于3人的现场驻场支持。

项目经理：本项目至少配置1名专职项目经理，项目经理具信息化专业领域高级工程师职称、高级信息系统项目管理师、CISP证书优先考虑，担任过政务云类似项目的项目经理不少于5年的优先考虑，提供项目经理的参与项目的经验清单（包括项目名称、服务时间、项目方、联系人等内容）。

技术负责人：本项目至少配置1名技术负责人，技术负责人至少具备CISP和高级信息系统项目管理师资质证书。

团队成员：团队成员不少于8人（含项目经理和技术负责人），具有政务行业信息化相关服务经验，提供团队成员参与过的项目经验清单（包括项目名称、服务时间、项目方、联系人等内容）。

# 服务提供方资质要求

1、符合《中华人民共和国政府采购法》第二十二条规定的服务提供方。

2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的服务提供方。

3、具有ISO9001质量管理体系认证证书。

# 安全服务内容

安全服务包括但不限于以下内容：

**1、等保测评：**应在项目验收前通过等保三级测评，并获取等保报告。

**2、密码应用安全性评估：**项目中涉及信息系统其安全等级保护在三级及以上且做过密码改造的，应在项目验收前通过密码应用安全性评估，并获取密码应用安全性评估报告。

# 应急服务

## 编制应急预案及开展演练

供应商应坚持主动预防、迅速高效的原则，紧密结合实际情况，在正式启动运维工作前完善应急预案，且在运维期内及时更新。

应急预案应包括但不限于以下内容：集成商应急处置组织架构；日常检查、隐患排查、风险评估和容灾备份等安全预防工作的时间、人员安排；预警响应方案，包括在不同等级应急响应下，相关责任人、处置人员队伍、外部技术支持、处置策略以及处置时间目标；应急处置方案，包括发现报告机制、集成商责任人职责、处置队伍组建、采取业务缓解、网络封堵、威胁追踪和现场取证等网络安全技术措施,以及阻断信息泄露、完整性检测、抑制影响范围、数据备份和恢复等数据安全技术措施；故障恢复预案；配合调查评估等。重要信息系统预案应增加协助舆 情管控措施等相关内容。

服务期内完成2次演练，基本要求如下：构建一个典型场景编制演练方案；编制演练脚本；开展演练培训；记录演练过程；形成演练总结报告。

## 应急响应要求

1、服务提供方坚持主动预防、迅速高效的原则，紧密结合实际情况，精心编制并持续完善应急预案。

2、服务提供方必须提供7\*24小时全天候应急响应服务。

3、依据故障时间及故障范围划分故障级别，故障级别分为四级，依次为Ⅰ级（紧急）、Ⅱ级（严重）、Ⅲ级（较大）和Ⅳ级（一般），分别定义如下：

Ⅰ级（紧急）故障为工作时间段（8:30——17:30）内大范围故障。

Ⅱ级（严重）故障为非工作时间段（17:30——次日8:30）内大范围故障。

Ⅲ级（较大）故障为工作时间段（8:30——17:30）内小范围故障。

Ⅳ级（一般）故障为非工作时间段（17:30——次日8:30）内小范围故障。

当：

a、发生Ⅰ级（紧急）故障后0.5小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应2小时内到达用户现场。

b、发生Ⅱ级（严重）故障后0.5小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应3小时内到达用户现场。

c、发生Ⅲ级（较大）故障后1小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应3小时内到达用户现场。

d、发生Ⅳ级（一般）故障后1小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应4小时内到达用户现场。

4、如发生故障，服务提供方应严格按照制定的应急预案中故障处理流程实施故障排除操作。

5、当故障排除操作全部完成后，服务提供方应向采购人提交运维故障报告，经采购单位验证通过后签字确认并归档保存，同时组织更新相关文档。

6、如遇有重大事件（包括汛期、节假日、政治军事活动等），服务提供方应科学编制安全保障方案，并根据采购人需要提供现场保障服务。

# 网络和数据安全管理要求

服务提供方在提供运维（运营）服务过程中应严格按照“同步规划、同步建设、同步使用”原则落实项目安全技术措施，将系统安全运营相关监控措施纳入方案。

若运维项目为涉密项目，服务提供方还须参考市保密部门管理要求，严格按照国家《中华人民共和国保守国家秘密法》等相关保密法律法规进行管理，并接受中心保密延伸检查。

1、在提供运维（运营）服务过程中，服务提供方应在中心限定的办公区域内、访问或使用中心限定的信息资产（包括但不限于场地办公设施、计算机、服务器等），并在规定的安全环境中进行数据处理、开发测试、运维监控等活动，遵守环境安全监控的要求，在开发测试工作中，不得使用真实生产数据、不得越级操作。

2、提供运维（运营）服务过程中若涉及开源软件、组件等产品的使用，服务提供方应在使用前向中心提供项目涉及产品的完整清单，并附相应产品的漏洞扫描报告、安全评估报告等证明材料，审核通过后方可使用。

3、服务提供方提供运维（运营）服务过程中须保障现有系统的网络通畅、系统可用和数据安全。严格落实网络和数据安全防护能力、密码应用、信创应用等运维、运营工作要求，配合开展系统等级保护定级、密码应用安全性评估等工作。

4、服务提供方在提供运维（运营）服务过程中，被中心或第三方测评机构检测出安全漏洞、等保/密评测评未通过，服务提供方须在规定时限内完成整改并提供复测报告，逾期未整改到位的有权按中心相关管理规定作出处罚。

5、服务提供方须提供自身的网络与数据安全管理制度、保密管理制度，并在中标后提供人员、财务及安全管理情况报告，发生造成中心及项目受影响的变动，应及时向中心报告。

6、服务提供方中标后与中心签订保密协议，同时服务提供方应对项目相关人员开展安全培训，并与该项目人员的签订保密协议，且保证用于项目实施工作的相关终端安装正版杀毒软件及防火墙。

7、提供运维（运营）服务过程中，服务提供方需要对收集到的所有信息严格管理，严禁在网络上传播、散布和出售，牟取商业利益；服务提供方人员不得以任何方式泄露、公开或传播项目涉及的内容及成果；不得非法篡改数据、非法入侵中心网络，不得影响数据的完整性及可用性；不得留存任何安全风险隐患；参与项目建设与质保、维修的个人，不得私自拷贝和留存上述信息副本。

8、指定专人负责项目实施过程中的安全工作，接受中心数据安全部门的直接管理和考核，协助开展安全检查等工作。

9、服务提供方若需互联网端功能测试，应经中心批准同意，结束后应及时关闭测试系统，删除测试数据，并将结果及时报备中心。

10、服务提供方通过项目获取到的中心数据禁止超过合同限定范围使用，以及违规转发第三方。

11、服务提供方应按中心规定申请数据服务接口，加强认证和鉴权防护，保护中心敏感数据不被泄露。

12、服务提供方禁止将管理后台、数据库服务端口暴露在互联网。

13、加强对项目人员的安全管理。进入项目前，项目人员应参加安全培训并通过考核，接受背景调查，提供本人无犯罪记录证明，与中心签订保密协议。入场前，项目人员应填写入场申请，按需申请系统账号、云桌面账号和工位。入场后，项目人员应在中心规定的安全环境中进行数据处理、开发测试、运维监控等活动，遵守环境安全监控的要求，禁止共用账号、拍照等。在开发测试工作中，依据要求将生产数据脱敏使用，禁止将生产数据导入个人电脑、将中心代码或敏感数据泄露或公开。禁止个人私自搭服务端和共享网络、终端跨互联网和政务外网。禁止在互联网传输中心敏感文件。非驻场人员，按需提出入网申请，并安装终端管理工具。禁止将中心数据在个人电脑上留存使用，因需求调研或设计获取数据的，禁止将中心敏感数据外发，或存储在共有云上，数据使用后应进行销毁。

# 网络和数据安全处罚措施

如供应商在服务周期内发生网络和数据安全工作违约情况，对中心系统造成网络安全或数据安全影响的，按照引发的安全事件等级和次数，中心将采取以下处罚措施，具体处罚措施由中心安全管理部门确定：

（1）限期整改。

（2）约谈企业负责人。

（3）扣除项目运维费用的1%-3%。

（4）上报主管部门，必要时终止项目合同并追究相关刑事责任。

供应商应承担服务过程中出现赔偿责任（包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费、保全保险费/担保费）。

实施分包服务的项目，由分包商产生的安全责任问题，供应商应与分包商承担连带责任。

事件类型与等级及与之相应的处罚措施详见附表。

# 备份与恢复

1、服务提供方须制定数据备份策略，定期备份关键数据。

2、服务提供方须制定数据恢复策略，以便发生故障时快速恢复。

3、服务提供方须根据实际情况制定相应灾难恢复策略，以便发生灾难时快速恢复。

# 项目的变更、解除和终止

如果服务提供方丧失履约能力、发生资不抵债或进入破产程序，招标单位可在任何时候以书面形式通知服务提供方终止本项目的执行而不给予服务提供方补偿。该终止本项目将不损害或影响招标单位已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

# 保密责任

1、中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标人不得对外泄露采购人要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

2、中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或中标人合作方违反保密规定，中标人应承担连带责任。

3、中标人（含中标人参与本项目的人员以及其合作方）未经采购人书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

4、以上内容的保密期限自中标人知悉保密信息起始至保密信息被合法公开之日止。

5、中标人对采购人提供的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信、邮件等发送,造成的一切后果由中标人负责。

运维过程中标人如出现失、窃密事情，参照网络和数据安全事件处罚措施同等处置，具体处罚措施由中心保密管理部门确定。

# 违约责任

1、因服务提供方违反保密义务或知识产权约定的，采购人有权要求服务提供方支付本项目费用总额不超过30%的违约金，违约金不足以弥补采购人损失的，采购人有权要求服务提供方赔偿超过部分。若服务提供方违反保密义务，采购人还有权立即单方解除维护服务合同而不承担任何违约责任。

2、服务提供方有下列情形之一，采购人有权解除维护服务合同：

（1）服务提供方在服务周期内出现重大网络与信息安全事故。

（2）因服务提供方服务质量问题导致采购人无法实现目的。

（3）擅自转让或者分包其应履行的义务的。

（4）违反或者未履行维护服务合同约定的其他相关义务，且在采购人要求的合理时间内未能纠正的。

# 关于转让和分包的规定

合同不得转让、分包。

# 网络和数据安全事件处罚措施

**网络和数据安全事件处罚措施**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类型 | 负面行为分级情况 | 追究措施 |
| 1 | 安全事件 | 1、发生网络安全事件或数据泄露事件，每发生一起，按不同级别进行追究。 | 见下 |
| 2 | （1）发生重大（Ⅱ级）及以上网络和数据安全事件的； | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的3%； 4、上报主管部门，必要时终止项目合同并追究相关刑事责任。 |
| 3 | （2）发生较大网络安全和数据事件（Ⅲ级）的； | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的2% |
| 4 | （3）发生一般网络和数据安全事件（Ⅳ级）的。 | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的1% |
| 5 | 2、被主管部门通报安全事件，每发生一起，按不同级别进行追究。 | 见下 |
| 6 | （1）被中央有关部门通报，并核实的。 | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的3% |
| 7 | （2）被本市有关部门通报，并核实的。 | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的2% |
| 8 | （3）被中心通报，对业务造成影响。 | 1、限期整改； 2、约谈企业负责人； 3、一个服务周期内累计发生3次及以上的，扣除项目运维费用的1% |
| 9 | （4）被重要用户投诉，影响中心形象、声誉。 | 1、限期整改； 2、约谈企业负责人； 3、一个服务周期内累计发生2次及以上的，扣除项目运维费用的2% |
| 10 | 3、在日常安全监控和检查中，发现服务厂商建设、运维的系统被非法登陆、信息泄露或篡改、病毒或黑客攻击等安全事件。 | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的2% |
| 11 | 4、在上级主管单位对中心进行安全检查中，发现问题的。 | 1、限期整改； 2、约谈企业负责人； 3、在一次检查中发现2个及以上高危问题的，扣除项目运维费用的2% |
| 12 | 5、未经批准，擅自在各种媒体发表与中心有关的评论或言论。 | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的2% |
| 13 | 故障 | 1、发生A1、A2级故障。 | 1、限期整改； 2、约谈企业负责人； 3、扣除项目运维费用的3% |
| 14 | 2、发生B1、B2级故障。 | 1、限期整改； 2、约谈企业负责人； 3、一个服务周期内累计2次及以上的，扣除项目运维费用的2% |
| 15 | 3、发生C+级故障。 | 1、限期整改； 2、约谈企业负责人； 3、一个服务周期内累计3次及以上的，扣除项目运维费用的1% |
| 16 | 漏洞 | 1、运维项目，未按要求上报产品漏洞情况，未及时更新版本 | 1、限期整改； 2、约谈企业负责人； 3、每发现一次未上报或未及时更新且存在漏洞发生安全事件的，按事件等级进行项目金额扣除。 |
| 17 | 2、存在漏洞风险，未按要求及时修复漏洞或采取防护措施 | 1、限期整改； 2、约谈企业负责人； 3、一个服务周期内累计3次及以上的中高危漏洞未按期整改的，扣除项目运维费用的2%； 4、每发现一次未按时修复且发生安全事件的，按事件等级进行项目金额扣除。 |