衢州市四省边际智算中心

建设指南

衢州市大数据发展管理局

2023 年 7 月 18 日

目录

1 引言

1.1 建设背景

习近平总书记在中央政治局人工智能发展现状和趋势第九次集体学习中强调，“人工智能是新一轮科技革命和产业变革的重要驱动力量，加快发展新一代人工智能是事关我国能否抓住新一轮科技革命和产业变革机遇的战略问题”。

衢州践行习近平总书记的殷殷嘱托，争创全省“两个先行”，力争把衢州打造成为四省边际高质量跨越式发展的中心城市。构建地市级智算中心，可为衢州打造四省边际数字变革桥头堡、高质量构建“跨省通”体系、推进政府履职核心业务数字化、加快推进数字经济发展和创新，提供强有力的算力和数据服务。

1.2 基础现状

衢州市四省边际智算中心，拟在市云计算中心政务云平台的基础上进行升级。衢州市云计算中心于 2018 年 3 月正式启用，目前政务云平台共有物理机 600 多台，网络及安全设备 128 台，共有 36471 核 CPU、143000G 内存、3865T 存储服务能力。

在过去的五年时间，市云计算中心政务云平台有效支撑了衢州市数字政府的高效运行，但在安全可靠、资源统筹、容灾备份及绿色集约等方面存在明显短板，平台亟需升级。

2 总体思路

2.1 指导思想

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大、十九届历次全会和二十大精神，深入落实国家、省、市关于加快数字经济发展的决策部署，以算力多元化、产业协同化、技术可信化、能耗低碳化为方向，全力推进四省边际智算中心建设，以实现新型基础设施、公共算力服务、产业生态创新等功能的集聚，为衢州市建设四省边际中心城市提供发展新引擎、树立新标杆。

2.2 总体目标

建设符合工信部《基于云计算的电子政务公共平台顶层设计设计指南》、《信息安全技术云计算服务安全指南》和《信息安全技术云计算服务安全能力要求》等国家及行业标准、规范的云平台。

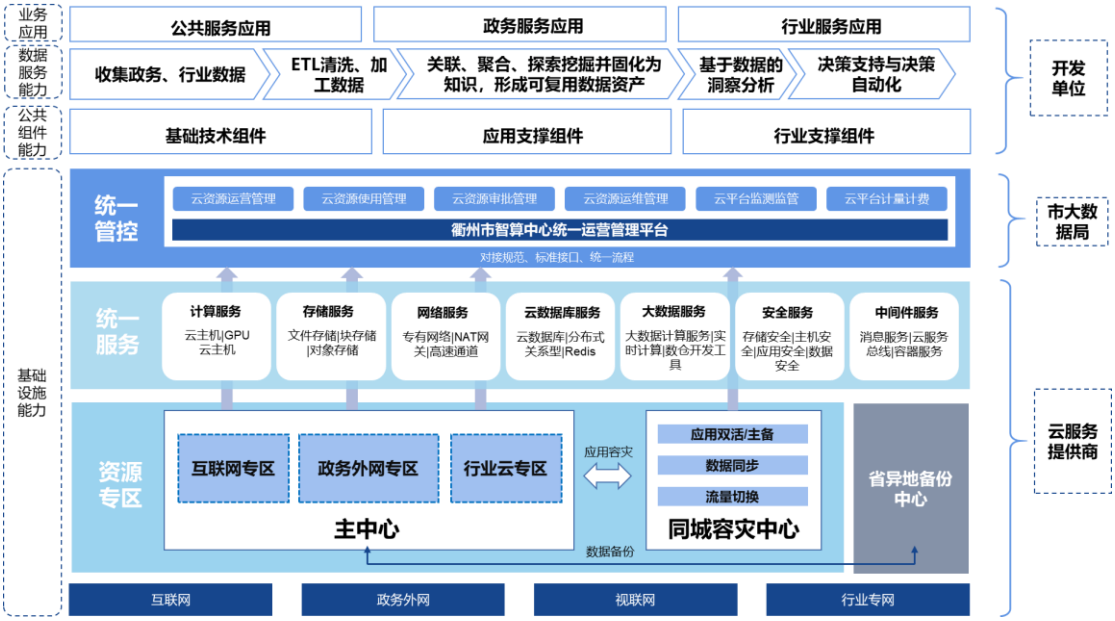
增强政务云、行业云、公共云服务支撑能力，满足政务、事业单位、企业以及公众上云服务的需求。

建设基于本地运营服务保障的云安全管理体系和运维管理体系，为入云应用系统稳定持续运行提供全面支撑。

建设完善的云服务监管体系，实现云服务（含安全服务）的集中可视化监控，通过监控平台展现服务运行状况。

3 总体设计

3.1 总体架构



总体架构如上：

云服务商提供云、网及相关云计算服务。网络层面包含提供互联网、电子政务外网、视联网、行业专网等网络服务。云平台资源区建设主中心和同城容灾中心。主中心包含互联网专区、政务外网专区、行业云专区。主中心与同城容灾专区按需实现应用级容灾（主备或双活），同时与省异地备份中心实现数据级容灾备份。基于资源专区实现统一云服务，包括计算服务、存储服务、网络服务、云数据库服务、大数据服务、安全服务、中间件服务等内容。

市大数据局建设市级统一云运营管理平台，通过标准接口对接各云区，实现统一云资源运营管理、云资源使用管理、云资源审批管理、云资源运维管理、云资源监测管理、云平台计量计费相关功能。

各业务开发单位基于以上云服务进行相关公共服务、政务服务、和行业应用的开发。

3.2 内容规划

衢州市四省边际智算中心包括三方面的建设内容：

建设安全可靠的政务数据中心。一是在硬件、平台、应用等三个层次实现政务云安可替代，在满足上级监管要求的同时，提升基础设施的安全可靠性。二是采用“两地三中心”的容灾架构提升政务云容灾备份能力，以保障政务信息系统数据安全和关键业务的连续性。三是通过资源调度、门户集成实现服务目录、资源供给、资源运营、资源运维和资源治理的统一服务，提升政务云资源的使用效能。

建设集约高效的行业数据中心。结合行业共性需求、数据服务、可控性与灵活性、完整性与开放性等特点，以公有云的建设模式、私有云的个性化标准搭建满足教育、医疗等公共服务行业需求的云计算平台，为上述行业提供数据资源内部聚集和共享服务，帮助相关行业数据拥有者将数据转换为服务，提升业务价值和服务能力。同时稳步开展行业应用上云部署工作，构建新型行业云集约运行和安全运营体系。

建设智能普惠的算力服务中心。通过人工智能操作系统、集群管理调度系统、AI 计算框架及开发集成环境、AI 能力软件等技术，构建融合通用计算、科学计算、人工智能计算于一体的公共算力平台和商业服务运营平台，实现资源、算力、运营的统一管理，面向企业数字化、人工智能、仿真建模、大数据计算等领域，为政府、企业、高校和科研单位提供全栈式的普惠算力服务，以降低整体业务运行成本、智算使用成本。

4 智算中心建设要求

4.1 基础设施建设要求

4.1.1 机房建设要求

项目		技术要求	备注
选址	距离停车场	不应小于 20m	包括自用或者外部停车场
	距离铁路或者高速公路	不应小于 800m	
	距离甲、乙类厂房，垃圾填埋场	不应小于 2000m	
	距离火药炸药库	不应小于 3000m	
	距离住宅	不应小于 100m	
环境要求	冷通道或者机柜进风区域的温度	18°C-27°C	
	冷通道或者机柜进风区域的相对湿度和露点温度	露点温度 5.5°C-15°C，同时相对湿度不大于 60%	
	主机房环境温度和相对湿度	5°C-45°C，8%-80%，同时露点温度不大于 27°C	
建筑	抗震设防分类	不应低于乙类	

与结构	主机房活荷载标准值（KN/㎡）	组合值系数中Ψc-0.9 8~12 频遇值系数中Ψf-0.9，准永久值系数Ψq-0.8	
	主机房吊挂荷载（KN/㎡	1.2	
	不间断电源系统室活荷载标准值（KN/㎡)	8~10	
	主机房外墙采光窗	不宜设置	
	防静电活动地板高度	不宜小于 500mm	作为空调静压箱时
	防静电活动地板高度	不宜小于 250mm	仅作为电缆布线使用时
	屋面的防水等级	I 级	
空气调节	冷冻机组，冷冻水泵，冷却水泵，冷却塔	N+X 冗余	
	冷冻水供水温度	7°C-21°C	
	冷冻水回水温度	12°C-27°C	
	机房专用空调	主机房中每个区域 N+X 冗余	

	蓄冷装置供应冷冻水的时间	n+X 冗余	
	冷冻水供回水管网	双供双回	
	冷热通道	隔离	
电气技术	供电电源	双重电源供电	
	变压器	2N	
	后备柴油发电油机	N+1 冗余	
	后备柴油发电机的基本容量	应包括不间断电源系统的基本容量、空调和制冷设备的基本容量	
	柴油发电机燃料储存量	满足 12H 用油	
	不间断电源系统配置	2N 或者 N+1 或者 1 路（N+1)UPS 和 1 路市电供电	
	不间断电源系统自动转换旁路	需要	
	不间断电源系统手动转换旁路	需要	
	不间断电源系统	15min 柴油发电机作	

	电池最少后备时间	为后备电源时	
安全防范系统	发电机房、变配电室、电池室等	出入控制（(识读设备采用读卡器)、视频监控	
	安全出口	推杆锁、视频监控、总控中心连锁报警	
	主机房出入口	出入控制（(识读设备采用读卡器)或人体生物特征识别，视频监视	
	主机房内	视频监视	
消防与安全	主机房	设置自动气体灭火系统	
	变配电、不间断电源系统和电池室	设置自动气体灭火系统	

4.1.2 网络建设要求

（1）智算中心互联网出口基本要求

智算中心云平台须为本项目租用的云主机提供公有 IP 地址，政务云网络的核心及出口基础设施要与政务外网匹配适应。

（2）智算中心与政务外网互联基本要求

须提供不同于其他运营商的传输专线进行互联（采用一主一备组网方式），用于智算中心平台与衢州市政务外网的网络互访，带宽不

小于 10G，符合政务外网建设规范。链路切换时延控制在 20-50ms 范围 。

4.2 云平台建设要求

4.2.1 自主可控建设要求

（1）智算中心应采用国产化芯片服务器搭建云平台底座，支持一云多芯、包含两种主流的国产化芯片；

（2）除采购方特殊要求外，政务云物理服务器扩容和替换须采用符合国家信创要求的产品；

（3）云服务器须提供符合国家信创要求的操作系统；

（4）如国家或省级信创产品采购认定技术标准出台，相关产品需配合完成认定申报。

4.2.2 云产品及服务建设要求

4.2.2.1 信创云产品及服务建设要求

智算中心信创云平台包含互联网专区和政务外网专区两个区域，云平台支持不同国产芯片架构的计算资源池，满足不同国产化应用替代场景。

智算中心信创云包含基础服务、存储服务、网络服务、云数据库服务、中间件服务、大数据服务、容灾备份服务、安全服务、统一云管平台服务、机柜租赁服务。

4.2.2.1.1基础服务

4.2.2.1.1.1云主机服务

云主机服务建设要求如下：

（1） 要求支持根据用户的需求动态的创建和分配计算资源与存储资源。

（2） 要求支持云主机创建，创建后，云主机已包含有操作系统，可立即使用，从创建到启动在 5 分钟以内。

（3） 要求云服务器提供快照制作，快照回滚，自定义 image，动态升级，可以为每块磁盘创建快照。支持设置自动快照策略。

（4） 要求支持虚拟机故障切换，在线迁移；支持宿主机宕机迁移。

（5） 要求主机之间网络访问逻辑隔离，支持创建和管理安全组；提供安全组的创建、修改、删除以及批量删除等功能。

（6） 要求提供丰富的 API 接口，包括资源的创建，删除，修改，查询，启动等操作。

（7） 要求云服务器工作节点采用分布式高可用架构（支持 HA 功能），保障云服务器的高可用性；支持资源独享模式，保障关键业务云服务器稳定运行。

（8） 要求支持虚拟机监控管理，提供性能监测分析、异常告警等功能。

（9） 要求支持资源调度，支持统筹管理集群中物理服务器的负荷情况，择优选择合适的物理机部署。

（10） 要求支持资源开通时指定 IP 地址。

（11） 要求支持故障切换，动态迁移，多数据备份等。

（12） 要求支持主流的国产化操作系统如：麒麟、统信等操作系统。

4.2.2.1.1.2GPU 云主机

GPU 云主机服务建设要求如下：

（1） 要求继承云主机功能及安全特性。

（2） 要求支持 GPU 直通，从容应对高实时、高并发的海量计算场景,可以将一块GPU卡直通给一个虚拟机,支持主流 GPU 的直通。

4.2.2.1.1.3块存储

块存储建设要求如下：

（1） 要求支持为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。

（2） 要求支持在线扩展容量，扩容期间无需关闭云主机，无需卸载云盘；系统盘在线扩容不停业务。

（3） 要求支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。

（4） 要求支持分布式 EC 和三副本数据冗余保护， 三副本模式下，数据三副本支持分布在 3 个机柜或 3 对接入交换机上。

4.2.2.1.1.4对象存储

对象存储建设要求如下：

（1） 要求支持基于三副本或 EC 校验模式的数据多重冗余备份，

保证数据安全。

（2） 要求支持 RESTful API 接口，通过开发工具包 SDK 或直接通过 RESTful API 进行对象存储操作。

（3） 要求支持 key-value 键值对形式的对象存储服务。

（4） 要求支持多用户隔离机制。

（5） 要求支持大文件的分片并发上传和下载，支持断点续传。

（6） 要求支持日志记录功能，方便追查访问来源以及进行多维度的统计分析。

（7） 要求支持标准 RESTful 协议的 API 接口以及多语言的 SDK。

（8） 要求支持服务端数据加密。

（9） 要求支持对象简单上传/表单上传/下载/下载到本地文件/删除/批量删除/复制/获取对象地址/上传任务的删除与取消/生命周期管理。

（10） 要求支持 Bucket/Object 级别的 ACL。

（11） 要求支持服务器端的加密功能，用户能够使用密钥管理系统上创建的密钥进行加密。

4.2.2.1.1.5负载均衡

负载均衡建设要求如下：

（1） 要求同时支持四层负载均衡和七层负载均衡。

（2） 要求支持集群高可用架构，支持动态扩展。

（3） 要求提供四层(TCP 协议和 UDP 协议)和七层(HTTP 和 HTTPS 协议)的负载均衡服务。

（4） 要求支持多种转发规则，满足不同业务场景的要求：域名、url 转发。

（5） 要求健康检查，提供后端 ECS 实例的健康检查。负载均衡服务会自动屏蔽异常状态的 ECS 实例，待该 ECS 实例恢复正常后自动解除屏蔽。

（6） 要求采用集群部署，可实现会话同步，以消除服务器单点，提升冗余，保证服务的稳定性。

（7） 要求支持轮询、最小连接数两种调度算法，轮询：按照访问次数依次将外部请求依序分发到后端 ECS 实例上；最小连接数：连接数越小的后端服务器被轮询到的次数(概率)也越高。

（8） 要求支持证书管理：针对 HTTPS 协议，提供统一的证书管理服务。证书无需上传到后端 ECS 实例，解密处理在负载均衡上进行，降低后端 ECS 实例的 CPU 开销。

（9） 要求支持会话保持功能。在会话的生命周期内，可以将同一客户端的请求转发到同一台后端 ECS 实例上。

（10） 要求支持访问控制，支持白名单访问控制。通过添加负载均衡监听的访问白名单，仅允许特定 IP 访问负载均衡服务。

（11） 要求管理节点采用全冗余架构。

4.2.2.1.1.6弹性公网 IP

弹性公网 IP 建设要求如下：

（1） 要求支持将 EIP 与 VPC 内的实例进行绑定，使该实例可以

与外网通信。

（2） 要求支持修改 EIP 带宽。

（3） 要求支持随时将 EIP 与实例进行解绑。

4.2.2.1.1.7国产 WEB 中间件软件

国产 WEB 中间件软件建设要求如下：

要求提供满足信创建设要求的主流国产 WEB 中间件产品。

4.2.2.1.1.8国产操作系统

国产操作系统建设要求如下：

要求提供满足信创建设要求的主流国产操作系统。

4.2.2.1.1.9国产数据库软件

国产数据库软件建设要求如下：

要求提供满足信创建设要求的主流国产数据库软件产品。

4.2.2.1.2存储服务

4.2.2.1.2.1文件存储服务

文件存储服务建设要求如下：

要求为云主机提供的低时延、持久性、高可靠性的数据文件级存储设备。

要求支持 NFS v3.0/4.0。

要求支持多个文件系统组成全局命名空间（可选）。

要求支持目录级容量 Quota 管理。

要求支持三副本或 EC 模式或 raid 进行数据保护。

4.2.2.1.2.2数据库存储备份服务

数据库存储备份服务建设要求如下：

（1） 要求支持主流数据库类型备份。

（2） 要求支持整个实例、多个数据库、单个数据库、多张表、单表、视图、存储过程、触发器、函数备份。

（3） 要求支持备份频率、周期、开始时间、并行线程数等备份计划配置。

（4） 要求支持全量和增量备份保留时长配置到期自动删除。

（5） 要求支持计划外手动发起全量备份。

（6） 要求支持恢复时间点配置以日历方式展示数据库可恢复时间。

（7） 要求支持恢复目标库可选新建实例或者使用已有实例。

（8） 要求支持恢复遇到同名对象可选择失败或重命名处理。

（9） 要求支持备份到三方存储池，包括文件存储、对象存储。

（10） 要求支持批量自动接入新增数据源实例。

（11） 要求支持相同的数据库类型和相同的备份类型的批量配置备份计划。

（12） 要求支持实时增量备份以及精确到秒级的数据恢复能力。

(13) 要求支持多种加密技术保护备份数据存储安全。

4.2.2.1.2.3表格存储

表格存储建设要求如下：

（1） 要求支持以实例和表的形式组织数据，通过数据分片和负载均衡技术，达到规模的无缝扩展。

（2） 要求支持单个毫秒级的单行平均访问延时。。

（3） 要求支持通过自动的故障检测和数据迁移，表格存储对应用屏蔽了机器和网络的硬件故障，提供高可用性。

（4） 要求支持灵活的数据模型：表格存储的表无固定格式要求，每行的列数可以不相同，支持多种数据类型(Integer、Boolean、Double、String、Binary)。

（5） 要求支持数据分区和负载均衡机制，数据分区系统均匀的调度到不同的存储节点上。

（6） 要求支持单机故障自动恢复：表格存储的存储引擎中，每个节点都会服务一批不同表的数据分区，这些分区的分布和调度信息由一个 Master 节点负责来管理，并且 Master 节点也会监控每个服务节点的健康状态。

（7） 要求支持支持私有 VPC 网络隔离，私有网络的实例。

（8） 要求支持多租户并行执行，租户任务提交到不同的队列执行，租户间资源隔离。

4.2.2.1.2.4日志服务

日志服务建设要求如下：

针对日志类数据的一站式服务，提供日志数据的采集、查询、分析、消费等多种功能。

4.2.2.1.3网络服务

4.2.2.1.3.1专有网络

专有网络建设要求如下：

（1） 要求在所提供的云平台构建出一个隔离的网络环境，客户完全掌控自己的虚拟网络，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等。

（2） 要求使用隧道技术达到与传统 VLAN 相同隔离效果。

（3） 要求支持按需配置网络设置、软件定义网络，管理操作实时生效。

（4） 要求支持使用高速通道实现跨地域/跨用户的内网互通和物理专线接入，支持使用 NAT 网关进行 DNAT/SNAT 转发。

（5） 要求支持 NAT 网关，支持灵活的 DNAT/SNAT 转发。

（6） 要求支持通过交换机将专有网络的私有 IP 地址划分成一个或多个子网。

（7） 要求支持根据业务需求配置虚拟路由器的路由规则，管理专有网络流量的转发路径。

（8） 要求支持自建 VPN 网关，弹性公网 IP。

4.2.2.1.3.2NAT 网关

NAT 网关建设要求如下：

要求平台提供 NAT 网关服务，支持 NAT（SNAT 和 DNAT）功能。

4.2.2.1.3.3高速通道

高速通道建设要求如下：

要求平台提供高速通道服务，用于在云上的不同网络环境间实现高速、稳定、安全的私网通信，包括跨地域/跨用户的 VPC 内网互通、专线接入。

4.2.2.1.3.4DNS 解析

DNS 解析建设要求如下：

（1） 要求支持 VPC 私有域名和全局域名转发配置管理和解析。

（2） 要求 VPC 私有域名解析支持租户隔离的功能特性，支持权威域名的添加、修改、备注、删除、批量删除操作的功能，同时也支持根据关键字进行模糊查询，针对每个 VPC 都可以提供定制化的私有网络 DNS 解析服务配置，实现 VPC 粒度的租户隔离功能。

（3） 要求支持全局域名的配置管理，满足所有 VPC 解析同样的域名数据的基础性需求，减少管理员的配置工作。

（4） 要求支持基于地理位置的全局域名调度和 VPC 私有域名调度，地域基于内网 IP 地址段的分配来标注，租户侧 DNS 云服务可以根据客户端访问的源 IP 判断地域，并把相同域名解析到不同的后端指定 vip 上，来实现基于地理位置的流量调度。。

（5） 要求支持内网权威域名管理和解析：支持 IPV6 域名解析服务。

（6） 要求支持域名主机记录的添加、删除和修改操作的功能，支持的记录类型包括 A、AAAA、CNAME、NS、MX 等。

（7） 要求支持对地址池内的地址值进行 TCP/UDP/HTTP/HTTPS/ICMP 等协议的健康检查。

（8） 要求支持域名级别的转发操作，将特定域名的解析操作转发到其他 DNS 服务器上进行解析；支持默认转发功能的配置，将本地不存在的所有域名的解析操作全部转发到其他 DNS 服务器上进行解析。

4.2.2.1.3.5VPN 服务

VPN 服务建设要求如下：

（1） 要求支持 SSL VPN 服务，支持通过 SSL-VPN 功能远程接入 VPC，修改 SSL 服务端的名称、本端网段、客户端网段信息，支持创建 SSL 客户端证书。

（2） 要求支持 IPSEC VPN 服务，支持 IPsec-VPN 建立专有网络（VPC）到本地数据中心的 VPN 连接，IPsec-VPN 支持 IKEv1 和 IKEv2 协议，同时支持 API 方式配置。

4.2.2.1.4云数据库服务

4.2.2.1.4.1云数据库-类型 I（兼容 Oracle）

云数据库-类型 I（兼容 Oracle）建设要求如下：

（1） 要求覆盖全迁移流程实现数字化迁移能力，包括但不限于：采集、迁移评估报告、JAVA 应用程序分析、目标数据库配置推荐、存储过程转 JAVA、全量 SQL 性能压测

（2） 要求提供从 Oracle 数据库向目标数据库的表结构及数据迁移的工具，提供从 Oracle 数据库向目标数据库全量增量迁移的支持，支持目标数据库反向同步至 Oracle 数据库，从而构建双向链路，实现持续对目标数据库的增量写入，最小化系统割接宕机时间。

（3） 要求支持 Oracle 兼容能力，包括：

支持对标 Oracle DBA_* / ALL_* 内置视图功能，包括 DBA|ALL|USER_TABLES、DBA|ALL|USERS_USERS、DBA|ALL|USER_VIEWS、DBA|ALL|USER_INDEXES 、 DBA|ALL|USER_PART_TABLES 、 DBA|ALL|USER_TAB_PARTITIONS、DBA|ALL|USER_TAB_SUBPARTITION

支持投标数据库到 Oracle 数据库的 dblink，dblink 至少支持查询功能

支持空字符串和 NULL 的常用操作，结果和 Oracle 保持一致

支持与 Oracle 一致的常见关键字别名使用方式

支持 FOR UPDATE 子句允许锁定所选行，并支持 wait n 和 nowait 功能

（4） 要求内置时空数据引擎，带有时间/空间位置信息的图形图像数据，用来表示事物的位置、形态、变化及大小分布等多维信息，支除支持与 OpenGIS 标准地理信息数据类型外，还

可扩展支持：几何模型、栅格模型、路径模型、点云模型、轨迹模型

（5） 要求至少支持 JDBC，ODBC，OCI，PHP，.NET 五种访问方式

（6） 要求是自主可控的 OLTP 集中式数据库软件，数据库厂商自研的数据库产品具有中国软件测评中心（工业和信息化部或其下属部门）出具的软件产品源代码溯源扫描评估报告，自主核心研发代码占有率高于 90%

（7） 要求软硬件适配能力：支持国产主流芯片服务器,包括但不限于飞腾、鲲鹏、海光等芯片，支持主流操作系统，包括 Redhat、Centos、Suse 等，以及国产操作系统麒麟、UOS 等；

（8） 要求产品生态开放，所投标数据库产品拥有投标厂商主导的开源社区，具备完善的数据库培训和认证体系,所提供证书官网可查，超过投标数据库产品拥有 15 个以上生态伙伴认证

（9） 要求在 OLTP 数据库领域获得过国家级科学技术类奖，或省部级科学技术类一等奖及以上奖项

4.2.2.1.4.2云数据库-类型 II（兼容 MySQL、Oracle）

云数据库-类型 II（兼容 MySQL、Oracle）建设要求如下：

（1） 要求支持数据库内部的加密存储、传输加密、访问白名单、Label security、安全审计、细粒度访问控制等安全特性

（2） 要求支持事务处理、MVCC 多版本控制、死锁机制，事务处理系统具备原子性、一致性、隔离性、持久性

（3） 要求兼容 MySQL、Oracle 常用语法和函数，支持 SQL92/SQL99/SQL2003 语法标准，覆盖 99.9%以上应用开发常用 SQL，包括存储过程、触发器、自定义函数、自定义类型等数据库对象。

（4） 要求支持标准 SQL 语法，支持数据的多数据分片/分区的自动路由与聚合，支持跨库的复杂查询

（5） 要求支持数据库集群多点写入、读写分离

（6） 要求具备在线全量备份、在线增量备份的功能，支持到任意时间点的备份还原操作，保证数据强一致、时间点强一致、不阻塞业务服务

（7） 要求支持大并发情况下的分布式事务，保证数据强一致和处理能力

（8） 要求提供图形化界面的数据库运维管理工具，具有可视化实时监控、自动化运维、报警、参数管理、集群管理、租户管理、日志管理、健康巡检等功能

（9） 要求软硬件适配能力：支持 x86、ARM 硬件平台、主流操作系统，包括 Redhat、Centos、Suse 等，以及国产操作系统麒麟、UOS 等；支持主流的中间件产品组件，包括第三方的中间件产品组件；支持主流编程语言访问接口，如 JDBC、ODBC、PYTHON、PERL、C#、OCI、Pro*C 等；支持主流的开发框架，如 Spring、Hibernate、MyBatis、JMeter、WebLogic 等；支持主流的应用开发连接池，如 Druid、C3P0、Tomcat、

HiKariCP、DBCP、CommonPool 等;支持异构芯片多集群混布，如同一个底座，可以同时部署 intel/海光/鲲鹏/飞腾，四个芯片的集群，复用同一套管控。

（10） 要求是一款具备高性能、高可用、可扩展的分布式关系型数据库。

4.2.2.1.4.3云数据库-类型 III（兼容 MySQL）

云数据库-类型 III（兼容 MySQL）建设要求如下：

（1） 要求采用全冗余架构，无单点故障。支持单 AZ 主备高可用架构，及同城 2AZ 主备高可用架构。支持共享存储架构，最大可支持单实例 32T 存储空间。

（2） 要求支持原生只读实例和读写分离功能，可支持不少于 5 个只读实例，自动实现读写分离以及读节点间的负载均衡。

（3） 要求提供完善的备份、恢复机制，支持手工备份和自动备份，支持物理备份和逻辑备份、逻辑备份支持库级备份，备份文件最长可以保留 730 天，并支持恢复到指定时间点。

（4） 要求提供数据库自主诊断、慢查询分析，提供全面的健康状态以便用户自动化运维。

（5） 要求提供用户可独有 CPU 资源选择的独享型规格，提供用户可独有整台物理机器的独占型规格

（6） 要求提供用户自服务门户和 API 接口：用户可自行创建不同规格的关系型数据库实例，并提供关系型数据库实例的在线扩容、备份、恢复、性能监控、异常告警、日志管理等功能。

（7） 要求支持业务无中断在线方式升级数据库规格及存储空间

（8） 要求支持对 MySQL 可视化日志管理，包括慢日志、错误日志、数据库主备切换日志等

（9） 要求支持虚拟专有网络和经典网络，可支持指定虚拟网络创建数据库实例。

（10） 要求产品可提供稳定可靠、可弹性伸缩的在线关系型数据库服务。

（11） 要求具备完善的安全防护措施，支持白名单设置、SQL 审计等功能。

（12） 要求支持数据 SSL 传输加密、透明数据加密。

4.2.2.1.4.4云数据库-类型 IV（兼容标准 SQL）

云数据库-类型 IV（兼容标准 SQL）建设要求如下：

（1） 要求采用基于 Share-nothing 的 MPP 架构，支持横向扩展

（2） 要求支持主备形态、分布式形态集群模式，支持基于裸机和云主机形态进行部署，为不同业务场景提供灵活的部署形态选择

（3） 要求支持分布式事务强一致，保障数据一致性

（4） 要求支持灵活的分区管理操作，降低分区管理复杂度，支持分区创建、修改、删除

（5） 要求支持表空间管理，表空间用于管理数据对象，与磁盘上的一个目录对应

（6） 要求支持大对象类型，包括 clob、text、blob 类型，其中 text

和 blob 支持最大 1G

（7） 要求支持生成 WDR 诊断报告，用于快速诊断数据库内核性能问题

（8） 要求支持完善的安全防护能力，包括全密态加密、透明加密、SSL 加密、动态脱敏

（9） 要求支持 Oracle 数据库到分布式数据库在线迁移和数据库实时同步的云服务。提供数据全量和增量迁移工具，降低了数据库之间数据流通的复杂性，有效地帮助用户减少数据传输的成本

（10） 要求设置已删除实例保留天数，可设置范围为 1~7 天

（11） 要求支持将删除的实例，加入回收站管理。用户在回收站保留期限内的实例可以通过重建实例恢复数据。

4.2.2.1.4.5Redis 数据库服务

Redis 数据库服务建设要求如下：

（1） 要求支持 string，hash，list，set，sortedset 等常见类型，支持事务和订阅

（2） 要求提供多种规格的缓存数据库实例，支持实例的创建、重启、释放、备份等管理操作，支持在控制台清除全部数据和清理过期数据；支持实例的网络隔离

（3） 要求支持主从、读写分离、集群等不同形态。

（4） 要求支持用户可以在不同形态之间进行切换且对外连接地址不变。

（5） 要求支持多线程版本，同等规格下提升实例性能。

（6） 要求支持实例会话管理，可查看会话列表，具体操作，执行耗时等信息，可对会话进行批量 kill 等管理操作。

（7） 要求支持缓存分析,支持查看 key 在内存的占用和分布信息。

（8） 要求支持大 key 分析。

（9） 要求兼容开源 Redis 协议标准、提供开源可靠的缓存数据库服务，基于双机热备架构及集群架构，可满足高吞吐、低延迟等业务需求

（10） 要求支持持久化机制，支持设置 AoF 落盘开关，保障数据丢失最小化

（11） 要求支持实例的手动和自动备份，支持自动备份策略设置，支持主从、集群版等多种形态实例的原地恢复。克隆实例，支持备份集下载。

（12） 要求支持多账号，支持设置读写、只读权限，最小化授权提供更高安全保障。

（13） 要求支持白名单设置，提供灵活的安全访问管理能力。

（14） 要求支持域名访问和域名修改，支持端口号修改，避免默认端口号扫描风险。

4.2.2.1.4.6分布式关系型数据库

分布式关系型数据库建设要求如下：

（1） 要求兼容 MYSQL 协议和语法，支持自动化水平拆分。

（2） 要求支持在线平滑扩缩容，服务能力线性扩展，透明读写分

离。

（3） 要求客户端支持：兼容数据库登录协议，支持 Workbench ，Navicat，SQLyog 等客户端。

（4） 要求提供的分布式数据库事务套件，实现最终一致性事务支持。

（5） 要求支持外部数据源的增量和全量导入，帮助用户实现数据库平滑上云。

（6） 要求支持分库分表按照逻辑库表导出。

（7） 要求提供 sql 命令的方式查看物理、逻辑架构，展示慢查询等功能，可以帮助迅速定位慢 SQL 问题。

（8） 要求支持自动化数据拆分，支持字符串，日期，数字的多种拆分方案。

（9） 要求提供完整的数据库运维监控系统，对数据库 IOPS，TPS，CPU 实时监控。

（10） 要求采用分布式集群服务，无服务单点故障。

（11） 要求支持存储层数据库白名单自动维护，通过白名单保证访问安全。

4.2.2.1.4.7数据库管理服务

数据库管理服务包含数据传输服务、数据库自治服务、数据管理服务。

数据传输服务建设要求如下：

要求提供数据迁移、数据实时订阅及数据实时同步等多种数据传

输能力。通过传输服务可实现不停服数据迁移、数据异地灾备、跨境数据同步、缓存更新等多种业务应用场景，构建安全、可扩展、高可用的数据架构。

数据库自治服务建设要求如下：

要求支持数据库自感知、自修复、自优化、自运维及自安全的云服务，帮助用户消除数据库管理的复杂性及人工操作引发的服务故障，有效保障数据库服务的稳定、安全及高效。

数据管理服务建设要求如下：

（1） 要求支持任务编排：支持任务编排按需定义多个任务节点组成 DAG 周期调度。历史执行 SQL 查询：支持历史执行 SQL 的模糊查询，可查看 SQL 执行的开始时间、数据库、SQL、状态、行数、耗时、备注等信息。图形化批量操作表：支持图形化批量操作表，包括批量清空数据，删除表，表维护（优化表、检查表、修复表、分析表），表名前缀（添加前缀、修改前缀）。

（2） 要求支持数据库管理工具，提供高效、安全、全面的数据库开发工作环境，支持多种数据库类型、多种环境统一的数据库 DevOps 研发流程解决方案。

4.2.2.1.4.8云分析型数据库

云分析型数据库建设要求如下：

（1） 要求支持细粒度的运行监控，包括 CPU 平均使用率、集群连接数、查询 QPS、查询响应时间、查询等待总耗时、写入

响应时间、写入吞吐量、写入 TPS、磁盘 IO 吞吐、磁盘 IOPS、磁盘使用量。

（2） 要求单集群同时支持 SSD 介质存储实例以及 HDD 介质存储实例。

（3） 要求支持分区数据生命周期自动管理功能，实现历史数据的自动清除。

（4） 要求是一种高并发低延时的 PB 级实时数据仓库，能够满足海量数据实时多维分析，快速处理万亿级别的大数据。

4.2.2.1.5中间件服务

4.2.2.1.5.1企业级分布式应用

企业级分布式应用建设要求如下：

（1） 要求提供应用开发、部署、监控、运维等全栈式解决方案，支持 Dubbo 或 Spring Cloud 等微服务运行环境

（2） 要求涵盖了应用生命周期管理、运维管控等众多功能。

（3） 要求支持弹性伸缩：弹性伸缩能够感知应用内各个实例的状态，并根据状态动态实现应用扩容、缩容。在保证服务质量的同时，提升应用的可用率。

（4） 要求支持限流降级：限流降级用于解决后端核心服务因压力过大造成系统反应过慢或者崩溃问题。

（5） 要求支持健康检查：健康检查对容器与应用进行定时检查和汇报，然后将结果上报到控制台，可以了解集群环境下整个

应用的运行状态，排查和定位问题。

（6） 要求支持灰度发布：灰度发布包括对单个应用的灰度发布和全链路灰度发布。通过灰度发布实现应用新、旧版本的平滑过渡。

（7） 要求支持生命周期管理操作。生命周期管理包括创建、部署、扩容、缩容、停止、删除等。因部署的集群类型不同，生命周期管理操作有些差异。

（8） 要求支持应用监控，在应用托管到分布式应用后，可以对应用进行监控。包括基础监控、服务监控、日志和通知报警。

4.2.2.1.5.2应用实时监控

应用实时监控建设要求如下：

（1） 要求支持基于数据集配置交互式大盘，大盘可动态刷新。

（2） 要求支持指定时间段内 NoSQL 调用次数统计，支持基于操作命令的调用平均耗时、调用次数的详情查看。

（3） 要求针对 Java 语言应用，支持通过探针方式提供应用监控，为 Java 应用安装 Agent 后，即可开始监控 Java 应用，无需代码侵入。

（4） 要求能统计出服务和服务的关联依赖图

（5） 要求可以查看该应用的所有外部调用的请求数、响应时间、错误数及 HTTP 状态码信息

（6） 要求支持应用接口的指标统计，包括请求数，响应时间和错误数等

（7） 要求支持对应用进行标签分组与过滤

（8） 要求支持默认提供应用各维度指标的报警，包括但不限于JVM、异常接口调用、应用调用类型统计、主机监控、数据库指标等应用监控的风险信息进行报警

（9） 要求支持基于用于自定义监控数据集指标的报警

（10） 要求提供对于服务提供者以及消费者的集群以及单机的CPU，内存，磁盘、网络的监控并以图形化形式按照小时，天，周进行曲线展现。

（11） 要求支持基于主流同步、异步调用框架，如 Spring Cloud, Dubbo（可选）, HTTP RESTful 的分布式链路跟踪。

4.2.2.1.5.3云服务总线

云服务总线建设要求如下：

（1） 要求支持 2 个云服务总线群组或实例之间的 HTTP 服务级联。

（2） 要求支持数据库协议、REST 协议，WebService 协议等广泛的协议支持，并支持各种协议之间做转换和互通。

（3） 要求支持简单数据转换和深度定制数据转换的不同场景需求。

（4） 要求支持服务总线节点的无间断扩容，能够水平扩展服务总线节点，线性增加服务能力。

（5） 要求可设置服务总体流量访问控制。

（6） 要求支持完整的针对服务链路和系统指标的日志、巡检和监

控。

（7） 要求可设置服务黑白名单，无需重启服务即可生效。

（8） 要求支持以 Web 界面形式进行 API 全生命周期管理，包括发布、订购、消费到注销。

4.2.2.1.5.4应用高可用

应用高可用包含流量防护和性能测试。

流量防护建设要求如下：

要求为应用和网关配置多种规则实现专业的流量防护手段、秒级的流量水位分布分析功能，保障业务的稳定性。

性能测试建设要求如下：

具备强大的分布式压测能力的 SaaS 压测平台，可模拟海量用户的真实业务场景，全方位验证业务站点的性能、容量和稳定性。

4.2.2.1.5.5消息队列

消息队列建设要求如下：

（1） 要求基于高可用分布式集群技术，提供消息订阅和发布、消息轨迹查询以及定时（延时）消息、资源统计等系列消息云服务，为分布式应用系统提供异步解耦、削峰填谷的能力，同时具备海量消息堆积、高吞吐、可靠重试等应用所需的特性。

（2） 要求支持 TCP 协议：提供更为专业、可靠、稳定的 TCP 协议的 Java 或.NET SDK 接入。

（3） 要求提供 Web 控制台：支持 Topic 管理、Group 管理、消息查询、消息轨迹、资源报表。Open API：提供 API 允许将 MQ 管理工具集成到用户的控制台（可选）。

（4） 要求支持消息类型：普通消息：消息队列 MQ 中无特性的消息，区别于有特性的消息。定时（延时）消息：允许消息生产者指定消息进行定时（延时）投递。事务消息：实现类似 X/Open XA 的分布事务功能，以达到事务最终一致性状态。顺序消息：允许消息消费者按照消息发送的顺序对消息进行消费。

（5） 要求支持大消息：支持 4MB 大消息（包含消息属性）（可选）。

（6） 要求支持消息查询：提供了三种消息查询的方式，分别是按 Message ID、Message Key 以及 Topic 查询。

（12） 要求支持运维管控：支持运维管理工具，方便管控平台集成以及统一运维。

4.2.2.1.5.6容器服务

容器服务建设要求如下：

（1） 要求提供容器服务（Container Service），一种高性能可伸缩的容器管理服务，支持企业级 Kubernetes 容器化应用的生命周期管理。要求容器服务简化集群的搭建和扩容等运维工作，整合虚拟化、存储、网络和安全能力，打造云端最佳的 Kubernetes 容器化应用运行环境。

（2） 要求支持集群管理：通过控制台 10 分钟一键创建 Kubernetes

集群。提供容器优化的 OS 镜像，提供稳定测试和安全加固的 Kuberntes 和 Docker 版本。支持多集群管理，支持集群升级和伸缩。

（3） 要求支持一站式容器生命周期管理：网络：提供优化的高性能 VPC/ENI 网络插件。支持容器访问策略和流控限制。存储：支持云盘、对象存储 OSS，提供标准的 FlexVolume 驱动。支持存储卷动态创建，迁移。日志：支持高性能日志自动采集和云日志服务集成。支持和第三方开源日志解决方案集成。监控：支持容器级别和 VM 级别的监控。可以和第三方开源监控解决方案进行集成。权限：支持应用级别的权限配置管理。应用管理：支持灰度发布，支持蓝绿发布。支持应用监控，应用弹性伸缩。

（4） 要求支持高可用调度策略，打通上下游交付流程。支持服务级别的亲和性策略和横向扩展。支持跨可用区高可用和灾难恢复。支持集群和应用管理的 OpenAPI，轻松对接持续集成和私有部署系统。

（5） 要求支持负载均衡，支持创建负载均衡实例（公网、内网）。容器服务的负载均衡方案支持原生的高可用负载均衡，可以自动完成网络配置的修改和更新。

（6） 要求支持存储，文件存储、块存储，提供标准的 FlexVolume 驱动。

（7） 要求支持镜像仓库，满足高可用，支持大并发，支持镜像加

速。

4.2.2.1.5.7API 网关

API 网关建设要求如下：

（1） 要求支持 HTTP2.0 协议、websocket、双向通信等

（2） 要求支持多种访问控制方式，包括 IP 访问控制、参数访问控制。

（3） 要求支持流量限制，包括基础流控功能，如基于授权的流量控制，流控的时间区间支持秒、分钟、小时。参数流控，支持从当前的请求或系统上下文中获取参数，并使用自定义的条件表达式对参数进行访问控。

（4） 要求支持参数映射，可以从 HTTP 请求的各种位置上读取参数，并支持映射到后端不同的参数名、参数位置上；错误码映射，支持将后端应答中返回的非正常请求，映射为客户端期望的错误应答的场景。

（5） 要求支持参数路由，从应答或系统上下文中获取参数，并使用自定义的条件表达式对参数进行逻辑判断，满足条件后，支持对后端服务的定义与覆盖规则。

（6） 要求支持自定义配置，包括按照后端超时、按照后端报错配置降级策略，及设置降级后的操作方式。

（7） 要求支持灰度发布功能。支持的灰度条件不限于：版本号判断、IP 地址、随机比例等。

（8） 要求支持大数据平台做为后端服务，以 API 形式对外提供数

据服务

（9） 要求覆盖 API 全生命周期管理，包括 API 设计、开发、测试、发布、运维监测、安全管控、下线等 API 各个生命周期阶段

4.2.2.1.6大数据服务

4.2.2.1.6.1大数据计算服务

大数据计算服务建设要求如下：

（1） 要求支持超大规模节点调度能力，具备单集群 30000 节点以上调度能力。为保证大数据集群具有高可扩展性。

（2） 要求采用分布式计算框架提供大规模数据存储与计算，可按需扩容。

（3） 要求支持 MapReduce 类型的分布式计算任务，支持 DAG 模式的作业处理方式。

（4） 要求支持多种计算框架如 SQL，MapReduce，Spark ，Graph

（5） 要求支持原生 Apache Spark 编程接口，用户可以使用 Spark 接口进行编程处理存储在大数据计算服务中的数据

（6） 要求提供完整 RESTful API 的方式提供离线数据处理服务，提供 JAVA SDK， Python SDK，等编程接口，支持 JDBC 接口等系列用户开发工具和接口

（7） 要求提供离线任务管理、监控告警的功能。

（8） 要求任务运维管理支持两种模式可供用户选择。

4.2.2.1.6.2实时计算服务

实时计算服务建设要求如下：

（1） 要求提供实时流数据计算服务的通用计算平台。

（2） 要求支持数据开发：提供全托管的在线开发平台，集成多种SQL 辅助功能。

（3） 要求支持数据运维：提供以下运维监控功能：作业状态、血缘关系和属性参数。

（4） 要求支持性能调优：支持手动和自动调优方式。

（5） 要求支持数据监控：对接云监控平台，提供实时监控服务。

（6） 要求支持强大的实时处理能力：单作业吞吐最高可达千万级别记录/秒，支持各类失败场景的自动恢复，支持多种内建的字符串、时间、统计等类型函数，精确的计算资源控制，彻底保证您的作业的隔离性。

（7） 要求支持良好的流式开发体验：支持标准 SQL，提供内建的字符串、时间、统计等各类计算函数。

（8） 要求支持不同账号间工作空间、业务逻辑、资源分配的相互隔离。

（9） 要求具备完善的权限认证，保证不同权限间的安全隐私。

（10） 要求提供流计算项目的分权管理并提供用户操作审计功能。

4.2.2.1.6.3大数据搜索与分析

大数据搜索与分析服务包含搜索服务、智能报表工具、实时数仓

服务。

搜索服务建设要求如下：

（1） 要求支持通过管控平台一键创建 Elasticsearch 集群、操作灵活便捷。

（2） 要求提供界面友好的海量信息索引库及全文检索集群运维管理平台，可实时查看索引库及集群状态，支持基础指标的 Web 化展示。

（3） 要求提供原生 Elasticsearch 的 API 编程接口，用于大数据搜索服务的数据导入，索引建立和数据检索。

（4） 要求数据入库后，支持通过插件兼容 SQL 查询，支持条件组合灵活查询。

（5） 要求支持分词器和词库的自定义扩展，满足个性化全文检索需求。

（6） 要求支持数据导入后实时分析和检索。

（7） 要求支持对海量全文数据库的结构化和文本关键词信息存储，进行多维度信息匹配及筛选过滤，倒排索引，全文检索。

（8） 要求集群规模可平行扩展。节点扩容过程平滑，不影响集群正常查询，不需要停服务。

（9） 要求提供一个分布式的全文搜索引擎，实现数据搜索、数据分析等功能。

（10） 要求支持业务创建和使用一个或多个 Elasticsearch 集群，具备较为完善的权限认证与隔离机制，保障数据安全。

智能报表工具建设要求如下：

（1） 要求支持多种图表。包含线图、面积图、柱图等图表组件。

（2） 要求支持下钻、联动、跳转、辅助线、趋势线、预测线。

（3） 要求支持电子表格，兼容 Excel 函数。

（4） 要求支持多工作空间权限、报表权限、数据权限、多门户权限可单独授权。

（5） 要求支持各类自定义 SQL 功能。

（6） 要求支持文件夹的新建、删除、重命名；支持数据集的新建、删除、编辑、新建仪表盘、新建电子表格、移动、复制等功能

（7） 要求支持常规关系型数据库和 hadoop 生态的数据库。

（8） 要求可以提供海量数据实时在线分析服务，支持拖拽式操作和丰富的可视化效果，帮助客户完成数据分析、业务数据探查、报表制作等工作。

实时数仓服务建设要求如下：

（1） 要求支持标准 SQL 语法（DDL，DML）

（2） 要求兼容 PostgreSQL 11 语法，及 PostgreSQL 协议客户端访问

（3） 要求支持基本数据类型：boolean、int、float、double、decimal、varchar、date、time、timestamp。

（4） 要求支持离线数仓的批量导入；支持流计算实时入库；同时数据也支持导出至对象存储。

（5） 要求支持数据按行存储或按列存储，提供面向海量数据进行多维分析与多表关联分析的能力，同时也支持高并发明细点查询。

（6） 要求具备数据生命周期管理功能，过期数据系统自动清理

（7） 要求提供交互式分析型数据库服务，与大数据生态无缝连接，支持高并发和低延时地分析处理 PB 级数据。

（8） 要求具备完善的权限认证，支持多级租户管理机制，多层账号管理体制，子账号管理。

4.2.2.1.6.4数据治理与分析

数据治理与分析建设要求如下：

（1） 要求为数据仓库/数据湖/湖仓一体等解决方案提供统一的全链路大数据开发治理平台。

（2） 要求支持多数据源之间的数据接入和同步。

（3） 要求通过 SQL 编辑器实现代码输入，包含关键字、函数、表、字段等信息；支持错误语法实时提示。

（4） 要求支持调度系统诊断，完善调度系统作业的性能和稳定性。

（5） 要求支持数据质量校验规则与调度系统结合，数据产出后立即触发任务调度，若配置的强规则校验失败，则将任务状态置为失败，避免脏数据对下游作业产生污染.

（6） 要求支持服务编排：提供拖拽式、可视化的服务编排能力，支持用户按照业务逻辑，以串行、并行和分支等结构编排多个 API 及函数服务为工作流。

（7） 要求支持分级管理：自定义数据安全等级。

（8） 要求支持数据脱敏：包含有敏感信息的数据库，对敏感信息进行动态遮蔽。

（9） 要求支持新建导出任务。要求提供实时流数据计算服务的通用计算平台。

4.2.2.1.6.5实时数据分发

实时数据分发建设要求如下：

（1） 要求单主题（Topic）最高支持每日 TB 级别的数据量写入。

（2） 要求提供开发 SDK 包，提供 Restful API 规范，用户可以使用自己的方式实现接口访问。

（3） 要求服务可用性不低于 99.5%。

（4） 要求提供企业级多层次安全防护，多用户资源隔离机制。

（5） 要求提供多种鉴权和授权机制及白名单、主子账号功能。

4.2.2.1.6.6大屏开发工具

大屏开发工具建设要求如下：

（1） 要求支持使用模板方式或者新建的方式创建可视化应用；支持对可视化应用重命名、拷贝分享、复制、删除、预览和发布。

（2） 要求可以按照名称、创建时间、修改时间这三种方式对已有的大屏进行排序，使大屏能够有序地排列展示，便于管理。

（3） 要求提供滤镜配置和画布图层搜索的功能。通过滤镜配置，

可以对大屏中组件的色相、饱和度、亮度、对比度以及透明度等颜色属性进行配置；通过画布图层搜索功能，可以对可视化应用中任何一个图层等进行搜索并快速定位。

（4） 要求蓝图编辑器内可配置数据处理类节点。数据处理内的逻辑节点包括并行数据处理、串行数据处理、序列执行和WebSocket。并行数据处理节点，是使用并行方式来处理多个事件，各事件之间互不影响。串行数据处理节点，是使用串行方式来处理一个事件。使用序列执行节点，保证动作从上到下依次执行。WebSocket 节点用于多端之间的命令和数据传输。例如大屏与移动端、大屏与触摸屏端的数据传输等。

（5） 要求通过智能主题功能，可以对大屏进行合理的配色，快速解决在设计大屏时遇到的配色困难的问题。

（6） 要求蓝图编辑器内可配置流程控制类节点。流程控制内的逻辑节点包括定时器、分支判断和多路判断。定时器适用于需要定时的场景需求，支持延迟定时、定点定时、循环延时定时和循环周期定时。分支判断节点属于 If-Else 判断条件节点，可使用在根据开关状态触发两个图层的显隐效果等场景。多路判断节点属于 Case-When 节点，通过对上游节点的输出结果进行判断，触发第一个满足条件的下游节点执行对应动作。

（7） 要求支持以下数据源：CSV 文件、API、静态 JSON、MySQL 数据库、PostgreSQL、SQLServer、SQLServer、Oracle、

Elasticsearch 等数据源

（8） 要求支持搜索、添加、收藏、成组、锁定、隐藏、复制等组件功能，支持组件的组内轮播

（9） 要求蓝图编辑器可通过导出和取消到蓝图编辑器、在蓝图编辑器内定位、显示或隐藏配置栏面板和蓝图编辑器画布上的一些基本操作，帮助快速使用蓝图编辑器并实现预期的组件交互功能。

（10） 要求蓝图编辑器内可配置多种逻辑节点。逻辑节点可以帮助设置组件和组件之间的交互逻辑，实现大屏内各个组件的交互。蓝图编辑器中包括全局节点、流程控制、数据处理和输入设备几种逻辑节点。

（11） 要求蓝图编辑器可通过可视化连线的方式，定义图层与图层之间的交互行为。通过配置蓝图编辑器的使用方法，帮助自由管理大屏中多个组件之间的交互关系。

（12） 要求可以将已经创建的大屏进行分组归类，使得大屏变得有序且功能性一目了然。

4.2.2.1.6.7机器学习

机器学习建设要求如下：

（1） 要求支持深度学习：提供深度学习框架（如 TensorFlow）。

（2） 要求支持自动调参：提供自动调参，全面降低算法使用门槛及算法使用者工作量。

（3） 要求支持算法市场：算法套件包括音视频预处理、特征工程、

模型训练及预测全流程处理，无需编程，拖拉拽构建视觉类处理流程。

4.2.2.1.7机柜租赁服务

机柜租赁服务建设要求如下：

（1） 要求提供独立综合机房，按需提供机柜空间，用以放置服务器、交换机、磁盘阵列、网络设备等。

（2） 要求电力供应保障:机房引入2路市电,配置柴油发电机组，市电油机可自动切换；机房具备单独电力室，配备400KVA(1+1)UPS。

（3） 要求的环境保障：机房内配置机房精密空调，可确保设备运行对环境温湿度的要求；配备完善的气体消防系统、防湿防水系统。

（4） 要求具备机房动环监测及报警系统、门禁系统；机房环境符合等保三级相关要求；机房通过绿色数据中心评估。

（5） 要求的运维值班:提供7*24小时机房运维值班及技术支持，对相关设备进行巡检、维护和监控（包括防静电、防火、机房内温湿度，对机器重启、监控网络是否正常），保障设备正常运行。

（6） 要求的日常管理：指派专人负责对机房人员及设备进出登记管理(人员与设备进出需经用户方审批同意),记录设备使用单位、人员及承载业务系统情况，建立相关台帐；每季度提

供运维报告。

（7） 要求的机柜使用率（设备占用U位除以机柜总U位，设备之间距小于或等于2U算占用）：每季度一次与托管设备单位确认更新在用设备及承载业务系统运行情况，及时下架未使用设备。

4.2.2.2 行业云产品及服务建设要求

行业云为衢州本地各行业按需提供本地化专属云+公有云资源服务能力。

智算中心行业云平台满足各行业资源需求即可。

4.2.2.2.1基础服务

4.2.2.2.1.1云主机服务

云主机服务建设要求如下：

（1） 要求根据用户的需求动态的创建和分配计算资源与存储资源。

（2） 要求云主机创建后，云主机已包含有操作系统，可立即使用，从创建到启动在5分钟以内。

（3） 要求云服务器提供快照制作，快照回滚，自定义 image，动态升级，可以为每块磁盘创建快照。

（4） 要求支持虚拟机故障切换，在线迁移；支持宿主机宕机迁移。

（5） 要求主机之间网络访问逻辑隔离，支持创建和管理安全组；提供安全组的创建、修改、删除以及批量删除等功能。

（6） 要求提供丰富的 API 接口，包括资源的创建，删除，修改，查询，启动等操作。

（7） 要求云服务器工作节点采用分布式高可用架构（支持 HA 功能），保障云服务器的高可用性；支持资源独享模式，保障关键业务云服务器稳定运行。

（8） 要求虚拟机监控管理：提供性能监测分析、异常告警等功能。

（9） 要求资源调度：支持统筹管理集群中物理服务器的负荷情况，择优选择合适的物理机部署。

（10） 要求支持资源开通时指定 IP 地址。

（11） 要求支持故障切换，动态迁移，多数据备份等。

4.2.2.2.1.2块存储

块存储建设要求如下：

（1） 要求支持为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。

（2） 要求支持在线扩展容量，扩容期间无需关闭云主机，无需卸载云盘；系统盘在线扩容不停业务。

（3） 要求支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。

（4） 要求支持分布式EC和三副本数据冗余保护，三副本模式下，数据三副本支持分布在 3 个机柜或 3 对接入交换机上。

4.2.2.2.1.3对象存储

对象存储建设要求如下：

（1） 要求支持基于三副本或 EC 校验模式的数据多重冗余备份，保证数据安全。

（2） 要求支持 RESTful API 接口，通过开发工具包 SDK 或直接通过 RESTful API 进行对象存储操作。

（3） 要求支持 key-value 键值对形式的对象存储服务。

（4） 要求支持多用户隔离机制。

（5） 要求支持大文件的分片并发上传和下载，支持断点续传。

（6） 要求支持日志记录功能，方便追查访问来源以及进行多维度的统计分析。

（7） 要求支持标准 RESTful 协议的 API 接口以及多语言的 SDK。

（8） 要求支持服务端数据加密。

（9） 要求支持对象简单上传/表单上传/下载/下载到本地文件/删除/批量删除/复制/获取对象地址/上传任务的删除与取消/生命周期管理。

（10） 要求支持 Bucket/Object 级别的 ACL。

4.2.2.2.1.4负载均衡

负载均衡建设要求如下：

（1） 要求同时支持四层负载均衡和七层负载均衡。

（2） 要求支持集群高可用架构，支持动态扩展。

（3） 要求提供四层(TCP 协议和 UDP 协议)和七层(HTTP 和 HTTPS 协议)的负载均衡服务。

（4） 要求支持多种转发规则，满足不同业务场景的要求：域名、url 转发。

（5） 要求健康检查，提供后端 ECS 实例的健康检查。负载均衡服务会自动屏蔽异常状态的 ECS 实例，待该 ECS 实例恢复正常后自动解除屏蔽。

（6） 要求采用集群部署，可实现会话同步，以消除服务器单点，提升冗余，保证服务的稳定性。

（7） 要求支持轮询、最小连接数两种调度算法，轮询：按照访问次数依次将外部请求依序分发到后端 ECS 实例上；最小连接数：连接数越小的后端服务器被轮询到的次数(概率)也越高。

（8） 要求支持证书管理：针对 HTTPS 协议，提供统一的证书管理服务。证书无需上传到后端 ECS 实例，解密处理在负载均衡上进行，降低后端 ECS 实例的 CPU 开销。

（9） 要求支持会话保持功能。在会话的生命周期内，可以将同一客户端的请求转发到同一台后端 ECS 实例上。

（10） 要求支持访问控制，支持白名单访问控制。通过添加负载均衡监听的访问白名单，仅允许特定 IP 访问负载均衡服务。

（11） 要求管理节点采用全冗余架构。

4.2.2.2.1.5弹性公网 IP

弹性公网 IP 建设要求如下：

（4） 要求支持将 EIP 与 VPC 内的实例进行绑定，使该实例可以与外网通信。

（5） 要求支持修改 EIP 带宽。

（6） 要求支持随时将 EIP 与实例进行解绑。

4.2.2.2.2网络服务

4.2.2.2.2.1专有网络

专有网络建设要求如下：

（1） 要求在所提供的云平台构建出一个隔离的网络环境，客户完全掌控自己的虚拟网络，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等。

（2） 要求使用隧道技术达到与传统 VLAN 相同隔离效果。

（3） 要求支持按需配置网络设置、软件定义网络，管理操作实时生效。

（4） 要求支持使用高速通道实现跨地域/跨用户的内网互通和物理专线接入，支持使用 NAT 网关进行 DNAT/SNAT 转发。

（5） 要求支持 NAT 网关，支持灵活的 DNAT/SNAT 转发。

（6） 要求支持通过交换机将专有网络的私有 IP 地址划分成一个或多个子网。

（7） 要求支持根据业务需求配置虚拟路由器的路由规则，管理专有网络流量的转发路径。

（8） 要求支持自建 VPN 网关，弹性公网 IP。

4.2.2.2.2.2NAT 网关

NAT 网关建设要求如下：

要求平台提供 NAT 网关服务，支持 NAT（SNAT 和 DNAT）功能。

4.2.2.2.3云数据库服务

4.2.2.2.3.1云数据库（Mysql\SQLServer）

云数据库（Mysql\SQLServer）建设要求如下：

（1） 要求基于高效的调度、备份、HA 控制、在线迁移以及监控系统，为用户提供为专业的云数据库服务。

（2） 要求支持关系型数据库的基本功能，并进行优化服务。提供数据库自主诊断、慢查询分析，提供全面的健康状态。

（3） 要求支持 SQL Server、MySQL 主流关系型数据库。

（4） 要求单数据库实例内存可达 96G，并发连接数可达 24000。

（5） 要求 MySQL 单数据库实例可创建的数据库数量达 200 个，用户数达 50 个。SQL Server 单数据库实例可创建的数据库数量达 20 个，用户数达 20 个。

（6） 要求采用全冗余架构，无单点故障，每个关系型数据库实例均实现主从热备。并提供完善的备份、恢复机制，用户可按需备份并恢复到指定时间点。

（7） 要求支持数据库在线升级、云内动态迁移、故障自动切换，实现业务秒级无缝切换，不中断用户服务。

（8） 要求按需开通，即开即用，按需计费，为用户提供方便的 Web

管理界面。

（9） 要求支持原生只读实例和读写分离功能，自动实现读写分离以及读节点间的负载均衡。

（10） 要求随着用户数和访问量的变化，可以弹性的调整数据库的规格，包含内存、连接数、IOPS、存储容量等，调整时服务不间断。

（11） 要求提供记录数据库的所有 SQL 访问记录的能力。

（12） 要求提供数据导入、导出工具，方便用户进行数据迁移。

（13） 要求提供日志记录功能，包括错误日志、操作日志、访问日志等，可追查访问来源以及进行多维度的统计分析。

（14） 要求具备完善的安全防护措施，支持白名单设置、SQL 审计等功能。

（15） 要求云服务端提供加密用户身份验证，提供不同的访问权限控制。

（16） 要求支持主流的数据库引擎，并提供完善的 OpenAPI 供外部调用。

4.2.3 容灾及备份建设要求

容灾及备份包含异地备份、容灾多活、传输专网、应用适配服务。

异地备份建设要求如下：

（1） 要求提供云服务器、对象存储、文件存储、关系型数据库备份能力；

（2） 要求支持自定义备份计划；支持创建、启动、停止备份计划；

支持备份日志、备份记录查看和图形化备份统计视图；支持按备份策略执行备份；

（3） 要求支持按备份记录或时间节点进行恢复；支持创建、启动、停止、和查看恢复任务；支持查看恢复实例的日志信息；

容灾多活建设要求如下：

（1） 要求支持同城多活容灾架构。

（2） 要求支持入口流量的精准引流和切流。

（3） 要求支持流量的统一接入,协议支持HTTP/HTTPS,支持按URI前缀回源到不同后端应用。

（4） 要求支持入口流量分流，支持两种策略：1）按比例分流 2）按业务属性分流。

（5） 要求支持数据库双活，支持数据库数据双向同步。支持数据质量保护，数据在路由计算归属的单元正常写入，在其他单元禁写从而避免脏写。

传输专网建设要求如下：

（1） 要求各容灾中心分别部署 10G 专线（裸光纤）

（2） 要求适配改造迁移容灾服务。

4.2.4 IRS 对接建设要求

4.2.4.1 运营管控服务要求

4.2.4.1.1 运营管理

1、云区与产品目录管理

针对 IRS 平台上衢州市云区、产品目录清单，需提供持续维护服务。

2、资源管理

针对衢州市政务云需支持申请、审批、开通、升降配、释放云资源的功能。实时跟踪申请单审批状态，追溯申请单内容。包含但不限于如下功能：资源查看、产品上下架、项目管理、资源管理、申请单查看、费用评估。

3、账单管理

针对衢州政务云资源账单提供系统化账单服务，支持自动化计量计费。须包含但不限于如下功能：月度账单、账单查询、账单确认、账单统计。

4.2.4.1.2 权限管理

1、统一权限管理

对用户进行分权管理，允许不同用户具有不同功能权限和数据权限。包含但不限于如下功能：多云用户整合提供统一认证、部门组织管理、用户管理等。

2、用户体系自管理

依托浙政钉部门与用户体系，管理云管平台用户角色和权限，支持部门管理员对部门内用户账号的自管理，支持系统账号打标，规避账号误删除风险。

4.2.4.2 IRS 对接管控服务要求

4.2.4.2.1 IRS 对接服务

1、IRS 政务云资源申请流程低代码开发与接口对接

在 IRS 流程引擎上实现云平台政务服务区与公众服务区 47 款云资源申请表单和流程开发，并与云管平台对接，用户可自助提交资源申请单，审批人员可通过移动端收到消息并反馈审批意见。

2、IRS 政务云资源升降配流程低代码开发与接口对接

在 IRS 流程引擎上实现云平台政务服务区与公众服务区 21 款云资源升降配表单和流程开发，并与云管平台对接，用户可自助提交资源升降配申请单，审批人员可通过移动端收到消息并反馈审批意见。

3、IRS 政务云资源释放流程低代码开发与接口对接

在 IRS 流程引擎上实现云平台政务服务区与公众服务区 43 款云资源释放表单和流程开发，并与云管平台对接，用户可自助提交资源释放工单，审批人员可通过移动端收到消息通知并反馈审批意见功能。

4.2.4.2.2 云资源开通管理服务

1、云资源自动开通

打通 13 款云产品的申请、审批与开通链路，与云底座控制台接口对接，审批通过即可自动开通，并提交自动回执。

2、云区对接

实现与各服务提供商云管平台的对接，获取资源使用、业务状态

等信息。不再收取各服务提供商云管平台对接费用。

3、应用与云资源对应关系维护

维护 IRS 应用与云平台项目、资源集对应关系，支持查询 IRS 应用关联的各类云资源，展示全链路对应关系。

4、运行可视化

提供面向资源效能、运行应急视角的 2 个可视化界面。

4.2.4.3 运营运维服务要求

1、政务云平台报告服务

定期提供面向大数据局的政务云平台运行报告、平台介绍报告等。

2、平台运维服务

服务厂商需定期对服务平台进行维护、巡检、问题扫描等，保障平台正常运行。

4.3 信息安全建设要求

4.3.1 政务云安全需求分析

4.3.1.1 政策合规需求

在云计算环境下，云安全定级对象至少包括两部分，一是云平台本身，需要平台服务商独立定级备案、过等保测评、密码测评；二是云租户信息系统，需要云租户独立定级备案。特别注意的是，云平台的定级不低于云上承载业务的定级。另外，云上开发的业务系统也应该独立定级备案、过等保测评、密码测评。

因此，在衢州云平台建设的同时，需要同步考虑安全各方面对网络安全法、数据安全法、等级保护合规、云计算服务安全能力要求的

满足情况。

4.3.1.2 一体化安全技术需求

政务云平台安全：对于衢州市政务云平台而言，对全网资产的统一管理是基础，只有资产明确，才能做好暴露面治理、统一运维、统一防护、统一监测、统一认证等防护能力，守牢云边界安全，建立可信、可靠的政务云服务平台，为云上系统提供安全可靠的运行环境。

云租户安全：对于云上系统而言，以等保和密评的合规建设为主要设计目标，提供云租户安全所需的基础资源，为衢州市政务部门及企事业单位的重要系统提供基础安全防护能力。

数据全生命周期安全：以智算中心的建设框架为基础，建立健全符合智算中心要求的数据安全能力体系，数据安全能力体系需围绕浙江省“一平台四横四纵框架”，建立涵盖数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据全生命周期管理的数据安全技术防护体系；同时围绕衢州市智算中心的运行要求，建立合法合规的容灾备份体系与运行管理体系，形成体系化的数据安全能力基础。

攻防实战能力：实战是检验网络安全建设成果的唯一标准，建立技术型、可量化的能力评价体系又是实战常态化的基础。随着 0day 攻击、APT 攻击、勒索软件等威胁愈发严重，安全对抗的水平不断提高，衢州市政务云安全建设逐渐由合规驱动转变为实战驱动。然而，传统的网络安全建设往往侧重于理论上的顶层设计，安全系统、安全设备能力大多依赖于安全厂商的维护，忽视了其在实战执行、实际运行中的有效性和滞后性可能，这导致安全体系落地上存在诸多瓶颈，如：

实战防护能力现状不清晰、实战防护能力建设缺乏指标指引、防护体系盲区难以发现。

4.3.1.3 安全管理制度完善与创新需求

随着数字化改革的推进，已经无法适用于基于大数据架构下的管理要求，也缺乏聚焦政务云安全方面的安全管理策略和制度规程，与之配套的安全管理规范及技术要求和指南等体系文件也相对缺乏。随着衢州市智算中心的建设，需要根据政务云安全、网络安全、数据全生命周期和业务应用等建立新的制度规范与策略流程。

4.3.1.4 政务云安全运营需求

政务云场景下针对资产和风险的安全运营管理涉及到用户的安全、合规和成本控制等多个方面，是各行业进行数字化转型不可或缺的一部分，以风险控制各个阶段为抓手，通过梳理制定运营规范流程制度的建设，为衢州市大数据局在数字化改革过程当中的安全运营工作提供有效的指引。通过安全监测与通报预警等安全运营技术支撑能力建设，确保公共数据共享交换以及大数据开放等应用在可管理、可监视、可预见的状态下运行，实现一体化监管监测、预警、通报、应急响应的联动机制。同时结合安全运营过程当中最重要的“人”的因素，整合碎片化的安全服务机制，让安全运营工作“有法可依”“有人执行”“有工具支撑”“有数据决策”。

4.3.2 政务云安全整体建设要求

4.3.2.1 建设目标

围绕政务云平台安全体系建设为工作核心，坚持“人防、物防、技防”的联防联控大安全理念，整合各方优势力量，推动多领域多专业交叉合作，依靠多角度、主动、被动防御等各种手段，覆盖数字政府基础设施、网络、平台、数据和应用等多个层面，形成良好安全生态体系，保障数字政府基础设施和信息系统平稳、高效、安全运转。建立数字政府建设的安全管理组织和体系；提升政务云、政务外网、政务数据资源、政务应用的安全防护技术；建立长效的安全运营体系；完善安全治理体系。

4.3.2.1.1建立体系化、实战化的云上安全防护体系

政务云平台作为数字政府建设的基础平台，其安全性直接关系到国计民生等正要业务的运转，因此以“实战化，体系化，常态化”为理念，以“动态防御，主动防御，纵深防御，精准防护，整体防护，联防联控”为举措，结合现在的网络安全形势环境，需要从政务云平台的资产、边界、暴漏面、租户等多个维度建立安全防护策略和模块，通过各个模块组件的分工配合、联动，构建全方位、多层级、一致性的网络安全防护体系，能够应对实战化的网络安全攻击。

4.3.2.1.2打造立体化、纵深化的租户防护技术能力

以政务云、政务外网、数据、政务应用为防护核心，构建技术支

撑体系，构建涵盖网络安全、数据安全、密码安全、业务安全等技术能力的多层防护体系。遵照《网络安全等级保护基本要求》（GB/T22239-2019）、《GB/T 31167-2023 云计算服务安全指南》、《GB/T 31168-2023 云计算服务安全能力要求》《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021），以《数据安全法》为核心，围绕《国家政务信息化项目建设管理办法》，综合考虑政务信息系统物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的安全、密码应用需求，设计合规、正确、有效的电子政务外网的政务信息系统的网络安全方案和密码应用方案，为租户网络安全等级保护合规，保障数据安全，通过密码应用安全性评估奠定基础。

建立健全数据安全管理制度，落实安全责任，为本地区本部门工作中收集和产生的数据及数据安全负责，同时采取相应的技术措施和其他必要措施，对个人隐私、商业秘密等敏感信息采取分类分级保护，保障数据安全，提升运用数据服务经济社会发展的能力，充分考虑等保测评、数据安全、密码测评对国产密码技术的应用要求，

4.3.2.1.3形成职责分明、边界清晰安全协同管理机制

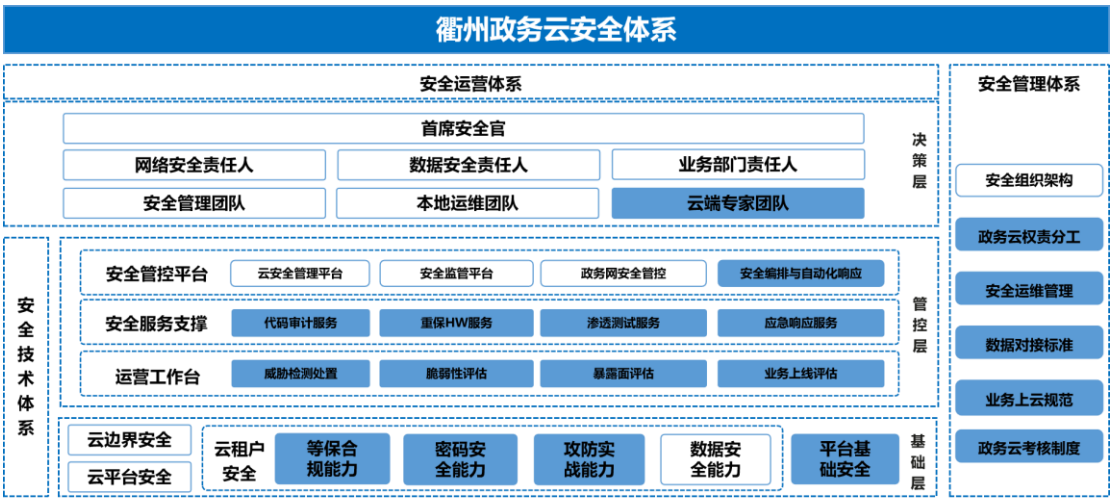
建立一套符合政务云平台的覆盖组织管理、内部管理、外部管理、服务商管理、制度规范的安全管理体系。组织管理方面通过大数据管理局及各委办单位安全领导小组、各安全服务商及系统建设服务商等，形成一套从领导层到管理层到执行层的三层体系，明确各方职责，为安全工作提供理论依据。内部管理方面依据各个单位安全管理委员会

机构职能，以关键信息基础设置和业务系统安全加固两类重要工作为基础点出发，明确政务云安全平台及服务商职责以及工作模式。外部管理明确政务云安全平台对各个委办单位的安全监测和通告的协同管理责任，以及各个委办单位对业务系统、政务数据、办公终端的主体责任。

4.3.2.1.4健全闭环化、流程化的安全管理运营能力

建立“监控—预警—响应—改进”的云上安全运营体系，对系统上云、数据汇集各类业务场景，形成一套行之有效的运营流程与配套的管理制度，驱动网络安全常态化运营。保证电子政务云平台的安全稳定可靠运行，更要保证租户的隔离，应用的互访，数据的流动，网络的通畅等一系列的关联问题。政务云平台的应用还与系统的等级保护，数据的分级保护，密码安全管理等各种信息安全和防泄漏、防攻击相关。因此，建立一个针对政务云平台和政务数据的安全体系，是政务云安全平台体系规划的重要目标。

4.3.2.2 总体设计



根据公安部“四新”要求和“六防”构建网络安全的新举措、新发展和新思路，按照衢州市数字政务安全平台体系建设的要求，以立足安全合规、面向攻防实战安全需求为导向，形成本次的政务云平台安全体系框架。整体建设理念采用预防性建设为主、检测响应为辅的思路，以“安全能力服务化，安全服务集约化”为设计原则。其次整体方案思路以合规为基线，以业务流程为导向，建立完善的网络安全保障和监管措施。引入高水平网络安全运营服务，有效支撑日常安全运营管理工作，将安全运营工作与各个支撑单位与组织联动起来，建立立体化的安全运营模式。技术路线层面围绕三大体系达成政务云安全全时域防护的目标，即技术体系、管理体系、运营体系。

技术体系：按照攻防实战的视角，将政务云平台的网络安全建设分为大边界安全、租户安全，分别对应云平台安全的南北向安全和东西向安全，为政务云平台及租户提供安全防护能力，其次为运营、管理决策等提供技术服务组件支撑。

管理体系：按照数字政府的建设规范及政策要求，健全安全管理

制度、安全管理人员等规范和台账等，形成本单位特色的管理体系。

运营体系：以立足安全合规、面向攻防实战安全需求为导向，参考 IPDRO 框架，将专业化人才梯队、标准化运营流程、智能化安全运营平台深度结合，从资产管理、攻击面管理、漏洞管理、威胁狩猎和应急响应五大核心攻防对抗域持续开展安全活动，助力用户建立安全长效机制，构建 7*24h 持续主动、动态调整、有效闭环的安全运营体系。

4.3.3 政务云安全具体建设要求

4.3.3.1 技术体系建设

4.3.3.1.1云平台安全建设要求

云平台安全防护区域是互联网与政务外网同时部署在各自区域内部上的安全防护区域。包括但不限于云防火墙、DDoS 高防、Web 网站实时防护、Web 安全监测、应用性能监测、网页防篡改、主机加固、云主机杀毒、云主机防御、数据库审计、日志审计等多款安全防护产品，且产品类型与数量应根据云服务使用单位的需求来增加或更改。

4.3.3.1.1.1安全域划分及区域隔离

通过对云平台进行网络安全域划分，可以把云平台这种复杂且大型网络系统安全问题转化为小区域安全保护问题，从而更好地控制网络安全风险，降低业务风险。同时，安全域划分的同时，可以理顺网络架构，对缺失的区域边界防护进行补充，更好的指导平台的安全规

划和安全设计。

4.3.3.1.1.2边界防护

边界访问控制：通过部署云平台边界访问控制设备，对进出云平台的流量进行精细化管理和控制，是云平台安全防护的第一道防线。

流量清洗：流量清洗的核心作用是防护 DDOS 攻击，保证云平台业务的连续性，由于 DDOS 攻击的特殊性，流量清洗设备一般部署在数据中心的最外层。对于云平台而言，同样需要配备流量清洗设备，防护针对云平台业务的 DDOS 攻击。

入侵防护：云平台承载业务具备复杂性和多样性，是攻击者主要的攻击目标，因此，在云平台边界需要配套部署入侵攻击防护设备，保证云平台的安全性。

流量检测（APT）：云平台上承载着重要的业务系统和核心数据，也是 APT 攻击的重要目标，并且 APT 攻击具有很长的潜伏期和持续性，会尽力隐藏自己的攻击和回连等行为，不易被发现。因此，需要在边界部署流量检测设备，分析进出云平台的数据流量，发现其中的攻击、回连、隐蔽通道等安全风险。

负载均衡：提供了有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

4.3.3.1.1.3安全远程接入

云上海量的应用和数据，存在着诸多的访问风险，因此远程接入的身份认证和访问控制是实现数据和应用安全的重要手段。对于云平

台的远程接入用户，平台侧需要提供安全可靠的接入方式避免不安全的远程接入带来的安全风险。传统的身份认证和访问控制措施存在维护困难、强度不足、实时性差等诸多问题，无法根据业务需求的变化进行动态演进，存在控制失效及影响应用开展的风险。需对云上业务进行身份认证及动态授权，以解决身份、凭证、访问和密钥管理问题。

4.3.3.1.1.4云平台主机安全需求

对于承载云计算资源的物理主机及虚拟主机，须实现主机的防病毒和入侵防御能力，保证病毒、蠕虫、木马等恶意代码一旦感染云计算主机，可做到及时检测发现、及时隔离、及时查杀，保证主机安全性。

4.3.3.1.1.5云内流量检测需求

针对云平台内部（东西）流量，需要部署流量检测分析设备，发现不同 VPC 之间的可疑流量和攻击流量，并第一时间做出相应。

4.3.3.1.1.6自身管理安全需求

平台运维审计：部署专业运维审计设备，实现对云平台的安全运维。

资产及脆弱性管理（风险评估）：全局掌握平台资产和资产脆弱性，并对脆弱性进行闭环管理。

平台安全监控：对平台侧安全能力进行集中监控，汇总各安全能力日志数据，全局掌握云平台安全风险态势。

4.3.3.1.2云租户安全建设要求

4.3.3.1.2.1等保合规

租户安全资源池整个各类安全组件，以解耦合或紧耦合部署模式为委办构建安全合规能力。此外，云租户安全体系还应以模板化的方式集成安全分析的能力，通过上述方案可以提供等保合规的安全能力，能力（包括但不限于）清单如下：

能力名称	实现能力	主要功能
堡垒机	提供云主机资产的运维审计功能，产品覆盖 SSH、RDP、VNC、Telnet、FTP/SFTP 等多种协议，支持通过浏览器 Web 页面和本地 C/S 客户端工具的方式访问主机，从而实现事前授权、事中监察、事后审计等完整的运维闭环	账号管理：集中管理所有服务器、网络设备账号，对账号整个生命周期进行监控和管理。
		身份认证：提供多种认证方式的统一认证接口，支持与第三方认证服务器结合。
		操作审计：审计账号使用（登录、资源访问）情况、资源使用情况等，并提供全方面的运维审计报表。
		资源授权：提供统一的界面对用户、角色及行为和资源进行授权，达到对权限的细粒度控制。
日志审计	通过对客户网络设备、安全设备、主机和应用系统日志进行	标准化日志：将各类日志统一进行解析识别，包括各种安全事件日志（攻

	全面的标准化处理，并进行全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，从而协助用户全面审计信息系统整体安全状况	击、入侵、异常)、各种行为事件日志（内控、违规)、各种弱点扫描日志(弱点、漏洞)、各种状态监控日志（可用性、性能、状态)。
		日志解析能力：采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理，同时支持多种解析方法（如正则表达式、分隔符、MIB 信息映射配置等）
漏洞扫描	集主机安全扫描、弱口令发现和基线配置核查于一身的检测类安全产品，通过提前发现系统的安全隐患从何帮助用户提高网络安全防护性能和抗破坏能力	主机扫描：主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。 高危漏洞、端口、弱口令扫描：信息系统存在的主机、软件的安全漏洞，安全配置问题，弱口令，不必要开放的账户、服务、端口，独创的端口
		基线核查：全面覆盖操作系统、数据库、中间件、防火墙、路由器、交换机等设备类型，支持 Windows 下的离线检查，无需一台台设备建立任务，一键

		提取系统配置信息，并可导入远程安全评估系统出具修复加固建议报告。
主机安全及管理（EDR）	提供主机系统防护与加固、主机网络防护与加固等功能，全面提升终端安全防护水平。	实现勒索病毒、挖矿病毒、已知（未知）病毒防护，提供安全监测、主机系统加固、元数据采集能力。
Web 云监测	提供漏洞监测、篡改变更监测、外链监测、挂马监测、webshell 监测等隐患监测、IPv4/IPv6 可用性监测服务、7*24 小时安全专家服务	
Web 云防护	为用户提供云端 Web 应用安全防护、入侵防护、实时攻击监测模块、防扫描、CC 攻击防护、一键关停、永久在线、安全防护报告、安全可视	

4.3.3.1.2.2攻防实战

主动防御（蜜罐）：实现重要应用系统主动安全防御。

威胁情报：针对云上业务安全风险，提供威胁情报平台，对云上安全设备的安全检测，云上告警的验证提供支撑。

APT 流量检测：针对一些高安全等级的安全区域，提供 APT 流量监测作为现有安全能力的补充，APT 流量检测能力可以通过现有运管平台下发到具体 VPC 内，实现 VPC 内的 APT 流量分析。

态势感知：实现具备全网流量处理、异构数据集成、核心数据安全分析、办公应用安全威胁挖掘等前沿大数据智能安全威胁挖掘分析与预警管控能力。为用户提供全局态势感知和业务不间断稳定运行安全保障。

4.3.3.1.2.3密码安全

租户安全资源池集成密码服务管理平台，提供包含密钥管理服务、安全通道服务等在内的九项密码安全服务，其安全能力主要由后台的密码服务平台、密钥管理系统、协同签名系统、传输透明加密系统、云密盾加密系统、数据库透明加密系统、签名验签系统提供。

委办单位可申请使用相应服务，根据负载动态调整基础密码设施的规模，实现密码运算资源的动态调整和灵活调度，为用户提供按需高效、弹性可扩展的密码服务，保证传输信息的机密性、完整性和有效性，确保设备和用户的身份真实性，同时平台密码服务设计分为密码服务层、密码支撑层、密码资源层以及密码管理后台。其中，三层服务构成从低到高的层级关系，低层可为上层提供密码服务支撑，密码管理后台作为密码服务的支撑与运维平台。

能力名称	实现能力	能力要求
基础密改服务		
传输加密服务	采用标准的国密 SM2、SM3、SM4 加密算法，为用户终端到云服务应用的访问提供数据加密传输能力。	B/S 架构，无集成改造、全流量加密传输加密速度：20Mb/s
		B/S 架构，无集成改造、全流量加密传输加密速度：40Mb/s，按月收费
		B/S 架构，无集成改造、全流量加密传输加密速度：80Mb/s，按月收费

		C/S 架构，需集成改造、字段级加密
存储加密务	支持对数据库进行表级别的透明加密、全字段以及敏感字段加密。数据最终以密文形式保存到业务数据库，实现信息系统内基本保护对象的加密存储保护，有效防止数据在存储环节的泄露风险。	1 个数据库，无集成改造、表级别加密。（需支持数据库插件安装），按月收费
		基于加解密模块（SDK）的封装，无需信息系统改造，实现数据存储加密，按月收费
		集成改造，字段级别加密，按月收费
安全运维通道服务（SSL VPN）	提供链路加密资源，满足用户多种基础安全需求，支持服务器之间数据传输安全、移动终端设备的接入安全等，为各个信息系统提供高强度的安全通道服务。	提供带国密证书的 key
https 国密认证	提供网页站点密评合规，绑定域名，支持国密+RSA	
国密浏览器	提供国密 SSL 协议和加密证书的浏览器	
高级密改服务		
数字签名服务	对数字签名以及验证接口进行封装，并按照一定接口规范提供给各个信息系统。信息系统通过	"实现对数据的数字签名和签名验证，签名速度：400 次/秒
		验签速度：200 次/秒，按月计费"

	调用密码服务平台的签名验签服务，完成对数据的数字签名和签名验证，并支持校验设备的身份真实性。	签名速度：1000 次/秒，验签速度：500 次/，秒按月收费
完整性校验服务	对国产数据哈希运算服务接口进行封装，以统一的服务接口规范向各个信息系统提供数据完整性保护接口。	实现数据的完整性校验，摘要计算速度：20M/s，按月计费
		摘要计算速度：40M/s，按月计费
		摘要计算速度：80M/s，按月计费
密钥管理服务	密钥管理服务包括密钥生成、分发、存储、使用、更新、归档、备份、恢复和销毁等全生命周期的管理。	支持 200 个用户，
		支持 500 个用户
密评的解决方案咨询服务	提供密码应用方案编制、密评问题答疑等，满足密码应用安全性评估对于密码应用方案评审的要求。	
安全管理制度服务	根据密评要求，协助梳理密码应用安全管理制度，建立操作流程与执行记录模版，制定应急处置办法并形成报告模版等。	

4.3.3.1.2.4数据安全

数据安全技术防护体系要求

- 数据库权限管控

数据库权限管控实现对内部技术人员的日常数据库操作行为进行权限控制，要求如下：

支持按需申请所需权限，支持数据库、表、字段或数据行级别的查询、导出或变更权限；

支持数据库实例的登录权限控制；

支持数据库操作的审计追溯。

- 数据库入侵防护

数据库入侵防护实现对外部的数据库攻击行为进行识别防护，要求如下：

支持 SQL 分析能力，对 SQL 注入行为进行识别并采取相应阻断策略；

支持数据库漏洞分析能力，对漏洞攻击行为进行识别并实时阻断攻击；

支持黑白名单机制，对白名单中的行为特征进行放行，对黑名单中的行为特征直接阻断。

- 数据库加密

实现主流数据库和云数据库存储加密能力，即使出现数据遗失、被盗的情况，也无法被解读出有意义的内容，从而减轻数据遗失所造成的损失。数据存储加密功能要求如下：

实现对用户数据的加解密存储与操作，通过云原生密钥管理服务实现秘钥管理，保证用户数据与秘钥的安全性。

支持以项目空间为单位，支持对全表数据进行加密存储。

数据加密后对用户使用保持透明，各种类型的任务不需额外改变，可以正常读取加密数据和非加密数据，项目空间内部支持加密和非加密数据共存。

- 动态脱敏

动态脱敏需支持敏感数据的脱敏能力，使用户的核心数据在日常业务中不会出现数据外泄的情况。要求如下：

支持数据脱敏规则设置，可灵活设置数据动态脱敏的具体规则、脱敏类型、脱敏位置等；支持数据脱敏白名单设置，设置白名单用户组，白名单用户组内的账号对数据的查询、下载不会被脱敏。

可根据不同场景配置不同的脱敏算法与规则，脱敏算法至少支持假名脱敏、HASH 脱敏、遮盖脱敏等多种脱敏则。敏感数据类型支持包括但不限于身份证、手机号、银行卡号、电子邮箱、车牌号、座机号、IP、MAC、姓名、地址、公司名等数据类型，以及所有通过数据字典识别的敏感数据。

- 静态脱敏

静态脱敏需支持敏感数据的脱敏能力，使用户的核心数据在开发测试等场景中不会出现数据外泄的情况。要求如下：

支持脱敏规则设置，在数据集成任务设置过程中插入静态脱敏规则、脱敏类型、脱敏位置；支持数据集成任务脱敏监控，可监控导出到特定存储的数据集成任务是否进行了静态脱敏。支持静态脱敏规则监控，可监控所有静态脱敏任务的具体规则，确认是否符合管理规定。

可根据不同场景配置不同的脱敏算法与规则，脱敏算法至少支持

假名脱敏、HASH 脱敏、遮盖脱敏等多种脱敏则。敏感数据类型支持包括但不限于身份证、手机号、银行卡号、电子邮箱、车牌号、座机号、IP、MAC、姓名、地址、公司名等数据类型，以及所有通过数据字典识别的敏感数据。

- 数据防勒索

数据防勒索提供对用户 PC 终端、ECS 服务器等操作系统的重要文件的勒索病毒防护能力，保障在遭受勒索病毒攻击的情况下的文件免受勒索病毒加密。要求如下：

支持黑白名单结合的形式对 PC 主机、服务器等文件进行保护，防止黑客通过勒索病毒对文件加密和修改来索要赎金。

支持文档防勒索，通过应用程序名、程序签名、安全标签（哈希值）等特征来描述一个具体的应用程序。

支持数据文件防勒索，仅允许授权应用程序读、写数据文件。

- 数据库审计

数据库审计以安全事件为中心，以全面审计和精确审计为基础，对数据库的各类操作行为进行监测、记录、分析，要求如下：

对监测到的审计日志支持生成审计综合报表。

对于监测到的风险事件，及时生成告警并以邮件、短信等方式通知相关人员，确保用户的系统符合各类法律法规对数据库审计的要求。

审计系统的运行对数据库系统和业务操作不应造成性能影响。

- 数据分类分级

数据分级分类通过自动化敏感数据智能识别、精准的数据分级分

类能力，提供对其敏感数据资产进行分类分级服务，帮助用户更好地管理好其核心数据。同时利用处理好的分类分级用于日常数据安全管理。

具备敏感数据识别功能，采取自动化识别敏感数据和分类分级打标，实现对政务数据的分类分级管理，并支持标准接口开放给一体化平台应用。敏感数据识别支持自定义的识别规则，提供基于关键词、正则表达式、数据表列名的敏感数据识别能力。

支持敏感数据的安全等级设定，支持通过可视化界面提供自定义安全等级设置，可灵活调整数据安全等级。支持敏感字段安全打标，可定期和实时识别敏感数据，根据分类分级结果对全量表及字段进行自动打标。

- 数据水印

数据水印为数据交换过程中发生的泄露事件提供追踪溯源能力，帮助用户更好的管理数据交换流程。

支持将水印嵌入到原始数据中，从而得到含水印的数据。嵌入水印后的数据保持与原数据类型和格式一致。同时需最大限度的保证脱敏后数据的特征一致性、逻辑一致性、业务规则关联性。

水印嵌入、数据溯源等操作均对用户不可见，整个水印过程黑盒化，防止监守自盗。

- API 审计

API 审计提供在以 API 作为数据交互的工具时的具体审计能力，帮助用户更好的管理 API 等接口的使用规范。

支持 API 识别能力，识别 API 的接口信息、参数信息、请求方法等。

支持单个 API 资产的访问次数、请求方法、状态、发现时间、活跃时间等审计内容。

- 文档加密

文档加密提供对用户终端中的文档进行透明加解密能力，管理终端电脑中的重要文档外发行为，控制外发文档的只读权限、绑定终端等方面的设置。

文档加密需满足透明加解密要求，使涉密文件只能在特定环境下进行使用。

具备解密流程审批能力，在文件使用者提出解密申请后，并由相关审批人同意后，对文件进行解密。同时审批流程及审批层级可自行定义，满足不同单位的审批需求。

数据安全容灾备份体系要求

- 业务系统容灾

业务系统容灾以云上用户的业务系统为单位，提供容灾能力，利用容灾中心的容灾能力，将用户在云上的业务容灾到容灾环境中，实现业务层级的容灾演练、一键切换。

业务系统容灾需具备数据库、应用、中间件等业务环境的容灾能力，并支持对容灾环境的实时监测能力，对监测到的异常环境实时告警。

满足容灾演练、灾难切换的业务需求，以快速拉起业务为第一优

先级，最大程度缩短业务停机时间。

提供切换指挥大屏，包括切换进展、耗时、切换日志流，并提供人工干预机制，最大程度保障灾难切换成功率，实现业务快速完整恢复。

- 数据库容灾

数据库容灾以云上用户的业务系统所属数据库为单位，提供容灾能力，利用容灾中心的容灾能力，将用户在云上的数据库容灾到容灾环境中，实现数据库级别的容灾演练、一键切换。

数据库容灾容灾需具备数据库环境的容灾能力，并支持对容灾环境的实时监测能力，对监测到的异常环境实时告警。

满足容灾演练、灾难切换的业务需求，以快速拉起数据库为第一优先级，最大程度缩短数据库停机时间。

提供切换指挥大屏，包括切换进展、耗时、切换日志流，并提供人工干预机制，最大程度保障灾难切换成功率，实现数据库快速完整恢复。

- 数据备份

数据备份采用数据备份和恢复技术，实现自动化数据备份和恢复，保障公共数据可用性和完整性，一旦发生公共数据丢失破坏或篡改事件，可利用备份数据及时恢复，支持任意时间点恢复。

提供租户视角的备份和恢复管理，云平台集成的备份管理，从租户和业务应用的角度来进行数据备份管理，用户可以通过制定备份计划，自定义备份周期来完成备份。通过创建恢复任务对已备份的实例

进行恢复。

支持云数据库备份恢复，支持 MySQL、PostgreSQL、SQLServer 等云数据库，支持无需安装备份恢复客户端的方式实现数据库实例粒度的备份和恢复，恢复策略支持新建型恢复方式，按备份记录或时间点恢复。

支持对象存储备份恢复，支持按 bucket 桶维度，无需安装备份恢复客户端，支持全量备份，支持永久增量备份，并支持按文件 prefix 匹配选定文件范围，恢复策略支持新建型恢复和覆盖型恢复两种恢复方式，按备份记录恢复。支持文件恢复规则设置只对某些文件进行恢复。

数据安全运行管理体系要求

- 数据迁移服务

数据迁移服务需支持以业务系统所在操作系统为单位，对操作系统进行整体迁移，保障迁移前后的操作系统所存储的内容一致。

数据迁移服务需支持以数据库为单位，对数据库进行整体迁移，保障迁移前后的数据库内容一致，为上云用户提供数据库从原有环境迁移至智算中心。

- 数据库监控平台服务

利用数据库监控平台，对数据库运行状态、监听、实例、表空间、SQL 执行次数、执行时间、数据库变化等参数进行实时监控并进行异常告警，为用户的数据库维护提供稳定可靠的技术支持。

支持对与数据库运行相关的参数进行实时监控。

提供监控大屏，显示数据库运行状态各项参数，如全局或指定业务系统的健康度、繁忙度、Top5 告警数、变更数、会话数、健康度等。

- 数据安全风险扫描发现服务

利用数据库漏洞扫描工具进行漏洞扫描，同时根据用户数据安全现状进行调研评估，结合漏洞报告和现状分析，从管理和技术角度对用户的数据安全风险进行评估，输出评估报告。

- 数据安全检查服务

基于数据安全能力成熟度模型（DSMM）等目标要求，从组织、制度、技术和人员维度，全面评估本项目的数据安全能力，对比数据采集、数据存储、数据传输、数据处理、数据交换、数据销毁六个周期对应的要求，分析用户的数据安全能力差距，进行全面的数据安全风险评估，并输出报告。

- 数据安全风险处置服务

依据数据安全风险现状及相关报告，配合用户对发现的数据安全风险进行处理，包括数据库补丁修复、安全策略优化、服务器协助加固等。

- 数据库运维及安全评估服务

对数据库进行运维安全评估，包括数据库巡检、运行状态评估，提供评估报告。

- 数据库高级运维服务

为用户提供全方位的数据库运维服务，要求包括 7*24 小时应急

远程响应支持服务、7*24 小时应急现场响应支持服务、灾难性故障应急支持、数据库性能优化、技术培训、数据库升级迁移割接等服务内容。

4.3.3.2 管理体系建设

4.3.3.2.1安全管理制度

建立健全“3+3”的政务云安全管理规范，形成一套全域体系化的制度规范，为政务云安全保障体系的落地提供法律依据和理论支撑，为开展日常安全管理工作提供依据、方式和方法，以规范化的流程指导政务云安全管理工作的具体落实

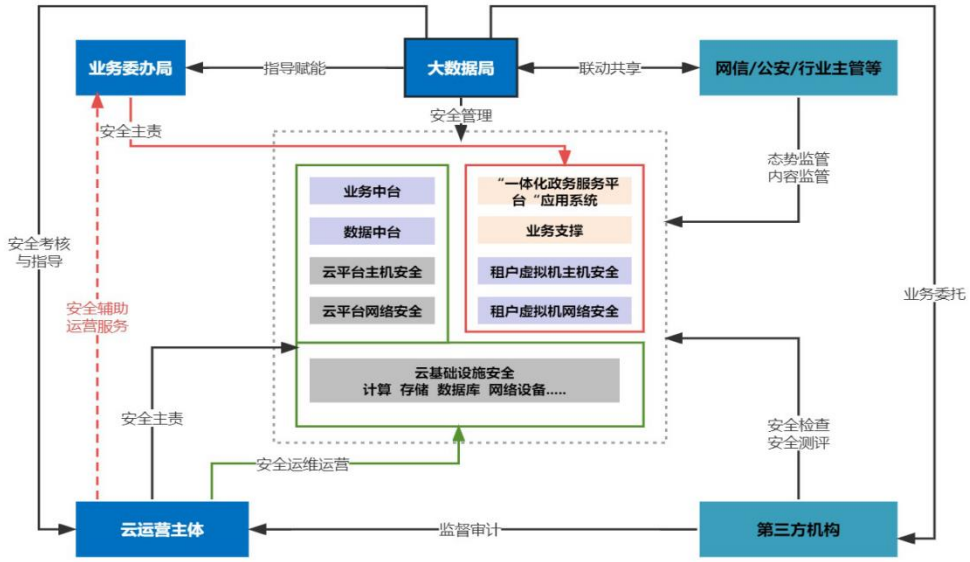
一级总纲：一体化安全管理总则一级文件为组织、方针，作为制度规范体系的整体指导（数据局）。包括《政务云权责分工制度》、《政务云组织架构》、《政务云安全工作责任考核制度》

二级制度：建立健全各单位开展日常安全工作过程的制度文件（数据局、网信、公安等）。包括《政务云应急响应处置制度》、《政务云安全运维制度》

三级规范流程：构建各单位具体业务环节进行规范、细化的操作规则、实施细则等（数据局、上云单位、云运营主体、第三方机构等）。包括《业务上云规范》、《数据对接标准规范》、《监测预警与应急处置操作手册》等

4.3.3.2.2安全权责划分

严格落实《党委（党组）网络安全工作责任制实施办法》及相关法律法规等要求，按照“谁主管谁负责，谁运行谁负责，属地管理”的原则，明确各参与方的安全权责，形成“多方参与、责任明晰、相互制衡、协同高效”的安全管控体系。



4.3.3.2.3安全管理机构

4.3.3.2.4安全管理人员

在安全管理人员方面，在人员录用、调动、离岗、考核、培训教育和外部人员访问管理几个方面，进一步加强及优化。

4.3.3.2.4.1人员录用

由组织最高领导层指定或授权专门的部门或人员负责人员录用，对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其

所具有的技术技能进行考核，与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

4.3.3.2.4.2人员离岗

及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，办理严格的调离手续，并承诺调离后的保密义务后方可离开。

4.3.3.2.4.3安全意识教育和培训

对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施，针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，定期对不同岗位的人员进行技能考核。

4.3.3.2.4.4外部人员访问管理

在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案，在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案，外部人员离场后应及时清除其所有的访问权限，获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。方面，进一步加强及优化。

4.3.3.2.4.5安全运维管理

根据组织网络安全管理制度体系框架中有关安全运维管理的制

度规定，利用物理环境、网络系统、网络安全防护等运行维护管理和监测审计的系统和功能，以及统一安全监控管理中心等，不断完善运维安全管理的措施和手段，强化运维安全管理的科学规范，具体包括：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络与系统安全管理、恶意代码防范管理、配置管理、密码管理、口令管理、变更管理、备份与恢复管理、业务上线一件事、安全事件处置、应急预案管理及外包运维管理等内容，确保系统安全稳定的运行。

重点要进一步建立完善网络系统安全漏洞的日常扫描、检测评估和加固，系统安全配置变更，恶意代码病的监测防护，网络系统运行的日志审计记录和分析，数据的备份和恢复，安全事件的监测通报和应急响应等机制，并注重对安全策略和机制有效性的评估和验证。

4.3.3.3 运营体系建设

项目服务保障的核心是人。对于保障运营来说，专业安全人员在安全运营体系中占据核心地位，合理地配置专业人员能够保证策略可有效执行、平台可有效使用、产品可合理管理、流程可正常运转。

项目服务保障过程中，采用三级梯队的服务构架，即一级梯队驻场人员提供标准化运营服务，二级梯队本地化服务团队远程专业支撑，三级梯队，总部团队专注专项安全研究和工具开发，以较低的成本共享高阶安全专家，实现安全问题的闭环解决。通过人将技术和流程有机结合，最大限度上发挥安全技术的价值，全面提升安全成熟度，实现安全能力最终落地和持续提升。本次项目安全服务保障团队。

4.3.3.3.1驻场运营团队

为保障政务云的正常运行，组建一支专业的网络安全运营团队驻场在客户指定场地。以“驻场人员总体牵头，专家团队在线支撑”的模式进行数据管理中心网络安全保障。安全运营团队组建以“能力多样、体系完善”为原则，打造一个能力全面、响应迅速的本地化专业技术服务团队。主场运营团队主要承担资产梳理和评估组、追踪溯源组、重保应急组等的运营服务工作，必要时总部将派人临时支撑，持续、动态、主动地落实安全运营工作。

驻场运营工作情况：

序号	驻场角色安排	主要服务内容
1	总牵头人	建立以政务云考核责任制为核心，负责组织实施、协调其他单位工作,主导工作任务
2	网络安全运维工程师	提供网络安全服务，要求包括 7*24 小时应急远程响应支持服务、7*24 小时应急现场响应支持服务、日常巡检、业务上线评估等工作。
3	数据库运维工程师	提供全方位的数据库运维服务，要求包括 7*24 小时应急远程响应支持服务、7*24 小时应急现场响应支持服务、灾难性故障应急支持、数据库性能优化、技术培训、

		数据库升级迁移割接等服务内容。

4.3.3.3.1.1监测预警要求

对安全平台上安全告警、安全事件、安全隐患结果进行分析核验，分离出误报，并对重点隐患、事件进行通报。具体职责包括：利用平台能力发现安全风险隐患后，向存在风险隐患的系统责任单位进行安全通报，将安全风险隐患问题进行统一梳理下发，实现安全风险隐患的统一安全管理。

4.3.3.3.1.2追踪溯源要求

发生安全攻击事件时能够根据现有的攻击痕迹追踪溯源，找到攻击来源和攻击手法。具体职责包括：把所有关注的网络安全需求数据集中统计分析，细粒度资产、系统日志、网络流量、进程行为、文件访问、账号访问等数据进行收集统计，建立正常行为模型，捋出异常数据，再进一步分析异常数据，发现其中的威胁，并复盘出存在的攻击链。

4.3.3.3.1.3问题追踪、整改复核要求

建立“问题追踪、整改复核”的云上安全运营体系，对系统上云、数据汇集各类业务场景，形成一套行之有效的闭环管理机制，驱动网络安全常态化运营。

4.3.3.3.1.4重保应急要求

在重要活动期间，全方位全天候防护与活动相关的单位，安排相

应的安全工程师进行 24 小时轮值安全保障、对单位系统、和网站、资产等安全状况，及时通报预警网络安全隐患，及时高效处置网络安全事件。在春节、劳动节、国庆节等法定假期和两会等重要活动时期以及重要活动时期，确保网络和信息系统的安全性、保密性、服务可用性。

（1）事前检查

在重要敏感时期，值守工程师进行事前检查工作，针对信息系统安全防护现状进行梳理，排查，包括：资产梳理、策略核查、基础安全扫描和查杀工作，针对重要业务系统根据用户需求进行其他安全检查测试工作，如：渗透测试，webshell 查杀等。

（2）流量监测

值守工程师根据部署在网络内的安全检测设备产生的告警信息，进行有效的及时整理、分析和处理。同时，对安全监控设备上的产生的告警日志信息进行有效的分析，形成对完全趋势的总体把握和了解，并根据相关告警信息对影响主机进行快速处理和响应。

（3）日志记录

值守工程师通过日志存储服务器全面汇总、存储由系统、应用和设备产生的日志记录，实现对日志记录的综合分析。日志记录都是由系统、应用或设备自己产生的，包含了有意义的数据和字段。在记录的时候，就已经可以做出初步的判断了。当然，更加复杂的“异常”判断还要提交到综合分析环节才能判定。日志是记录在服务器上发生的一些事情，也是对事件的一种检测。

例如：服务器的LOG、客户端管理的日志记录、各种应用系统的LOG、流量异常检测-sflow/netflow、综合日志审计平台、安全设备日志。

（4）主动扫描

值守工程师定时定期对被保护目标进行安全检查，包括对是否存在正常运行风险的分析，并且形成相关报告提交客户，商议得出解决办法。并根据扫描结果分析目前客户安全状况，并与客户沟通了解客户业务运行状况。

例如：漏洞扫描器、病毒扫描、服务器检查、基础渗透测试。

（5）搜索核实

当发生安全事件时，值守工程师利用搜索及时了解攻击相关技术环节内容，了解攻击者的来源，取得相关现场的数据证据，同时与客户确实核实是否对业务产生影响。

搜索核实一般都由用户发起，值守工程师协助客户完成相关安全检查，这里的判断基本上依赖于人的感觉和判断。对于呈现在眼前的东西，经过人的判断后，提交举报，这里检测出来的是结果和对于结果的一个判断既可以使一个发生的事件也可以是对于某些客体的状态判断。

例如：抓包分析工具、现象验证。

（6）汇总分析

各方面数据汇总在一起，分析判断需要知识库作为第一步初选，然后再由值守工程师作出分析判断。其中由监控形成的每日事件统计，

以及由每日事件统计报告形成的安全事件基线作为在突发事件发生时的重要判断依据。

4.3.3.3.2云端专家团队

通过远程安全专家团队提供咨询服务以及7*24小时事件应急响应服务，主要工作内容包括：威胁监测与持续响应、安全事件/漏洞验证/脆弱性识别、安全策略、安全告警分析、疑难日志分析、安全威胁溯源/疑难故障处理、安全效果运营/威胁模型构建、安全体系设计等。提供7*24小时远程技术支持服务，提供重要时期云端值守服务；提供互联网资产暴露面检测服务，以攻击者视角出发进行攻击面管理，挖掘最容易被攻击的应用指纹、高风险可利用漏洞；根据威胁监测服务，组织具有丰富经验的网络安全情报分析人员，提供对全市网络安全重点事件的专题分析服务，并结合威胁情报优势以及中心运营团队能力，提供规则关联分析、情报关联分析、行为分析、威胁狩猎多种威胁检测技术手段，实现对各类威胁的高效检测；服务人员结合安全知识库（持续积累了海量的安全告警分析、处置、攻防对抗等知识）提供的案例和安全建议，迅速判定安全威胁并完成快速响应；每季度安全运营专家现场进行阶段工作汇报，确认，沟通后续运营重点工作方向，并对安全设备的安全策略进行统一优化工作；为政务云建设提供主动防御、威胁溯源、攻击分析、发现失陷等能力，为业务稳定、安全运行提供核心支撑。

4.3.3.3.3安全运营平台

4.3.3.3.3.1网络安全态势感知

安全态势感知是用来向用户提供政务云网络安全威胁可视化的入口，实现预警通知效果，并对其范围、类型、危害以图形化展示，为安全分析人员提供直观、强大、清晰的安全威胁预警能力，以及重大问题、事件的整体性报告，实现安全事件自动化响应，形成威胁发现、智能研判和响应处置的安全运营闭环处置流程。

网络安全态势感知需具备态势感知、多源数据采集分析、资产梳理、分析建模、研判处置、通报预警等能力。

4.3.3.3.3.2数据安全态势感知

数据安全态势感知通过收集各种安全数据，基于专业的安全分析模型，将各种安全事件进行可视化呈现，准确、高效地感知防护对象的安全状态及变化趋势，结合分析、研判、预测技术，专注风险的分析、发现、评估和可视化能力，为数据安全运营提供可靠的信息数据支撑。

数据态势感知需具备日志采集、日志处理、关联分析、风险感知等能力，并提供分析模型，为数据安全事件研判提供正确有效的态势数据。

提供数据安全态势、设备态势、风险态势等安全大屏，直观展示用户现阶段的安全现状。

4.3.3.3.3.3统一运营管理平台对接

根据衢州市大数据局发布的《平台接口标准》、《数据规范标准》，各平台开放标准接口进行数据对接,态势感知大屏数据接入衢州市智算中心统一云运营管理平台。

4.3.3.3.4本地团队运营服务

4.3.3.3.4.1脆弱性评估管理

脆弱性评估管理服务通过配置核查、漏洞扫描、渗透测试、人工核查等手段探测和识别资产存在的脆弱性问题；待评估结束后，针对发现的安全问题，提供加固建议，协助相关业务部门、建设部门、管理部门、运维部门等评估安全加固方案;通过脆弱性管理,开展通报、复测等工作，定期跟踪修复工作进展，实施系统上线检查流程；通过协助加固方案验证，落实加固举措；通过上线检查流程，对即将上线的系统进行脆弱性评估和安全合规检查,以发现脆弱性问题和不合规项，并依据合规要求提出整改建议协助安全加固，出具系统上线安全检查报告。

4.3.3.3.4.2威胁事件监测处置

威胁事件监测处置通过部署必备的安全运维组件、安全设备，对流量、日志进行全方位监控分析，基于其产生的威胁事件告警、异常行为日志，利用剧本编排、自动化响应与大数据分析技术，在海量安全告警和日志中对各类疑似安全事件的告警进行监控分析、研判溯源、

响应处置，分析所面临的潜在风险，先确定安全事件的真实性，再进行事件预警通报，通过对安全事件进行实时分析、深度分析、威胁溯源，提供相关建议举措并协助用户及时进行处置，降低事件带来的损失和影响。

4.3.3.3.4.3应急响应与处置

应急响应服务通过项目经理和相关技术人员第一时间了解事件发生情况，判断事件类型，确定事件发生情况，与相关人员确定是否启动应急响应服务。在启用应急响应后，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的时间、现状、可能的影响，对事件采取取证分析、样本分析、溯源分析、问题追踪、证据收集、处置复核等手段形成攻击画像，提供事件处置建议，并协助相关人员解决事件；待事件处理结束后，撰写应急响应服务记录报告并提交。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作，对本次应急响应事件的发生进行复盘，以提升应急效率，完善运维方案、安全防护策略、安全管理制度、流程。

4.3.3.3.4.4安全应急演练

在政务网内，针对运行环境安全、网络结构安全、设备运行安全、系统可用性、外界风险因素等各方面进行全面演练，主要覆盖重要信息系统、数据中心、灾备中心等重要基础设施，重要服务商应急保障能力，外部应急协调机制等。选取适合大数据局应急环境开展应急演练工作，通过组织单位应急响应人员了解信息安全应急预案的目标和

流程，熟悉应急响应的操作规程，提高应急处置能力，明确相关单位和人员的职责任务，理顺工作关系。做到相关应急人员应知应会、熟练掌握、迅速反应、正确处置。

4.3.3.3.5高级专家运营服务

4.3.3.3.5.1资产发现与资产管理

理清资产是用户提升安全运营能力的第一步，同时也是最基础的一步，如果不清楚自身的资产情况，后续的安全建设都无法从全局进行考虑，因此在资产工作上主要由资产发现工作和核心资产管理两项工作。

4.3.3.3.5.2暴露面检测与攻击面管理

网络入侵的起始阶段，黑客会在前期针对目标单位、以及目标子单位进行全面的信息搜集如：子域名、c 段、c 段开放资产及服务、web 组件、web 中间件应用、组织架构、备案信息、邮箱信息、通过前期进行资产发现，黑客会优先选择薄弱的资产或者社工的方式利用漏洞直接获取相关应用/终端的权限。这个过程一般叫做“打点”，当突破口子之后，黑客会进一步入侵进行建立稳定的内网隧道，黑客搜寻到的全部信息即可理解为暴露面，最容易被选择突破的入口集合称之为攻击面。

互联网暴露面检测与攻击面管理服务，依托云端托管运营服务平台的检测功能，从攻击者视角自动对组织资产周期性监控并对互联网

资产暴露面的边界梳理，对互联网暴露面资产梳理开展一次“大体检”，摸清组织互联网资产底数，实时感知网络资产的安全态势，并以红队的视角筛选出最容易被黑客攻击的攻击面，协助组织将一些高危攻击面优先进行管控，如通过访问控制、关闭互联网访问、减少高危端口等手段，减少不需要的攻击面减低入侵风险，提高效率的同时也满足组织内部自查、上级核查和行业普查的安全需求。

4.3.3.3.5.3持续安全运营服务

持续安全运营工作主要包含“安全运营健康度评估”和“定期上门汇报交流”两大工作项，其价值在于，每季度平台生成的安全运营健康度评估报告可直接展示服务一定阶段后的效果，也可作为网络安全保险承保参考依据。同时，每季度安全运营经理现场进行汇报阶段服务进展、确认是否调整服务核心资产，都有利于服务专家更了解用户在下个阶段运营工作项重点的需求。

4.4 绿色低碳建设要求

衢州市四省边际智算中心通过使用浸没式液冷散热、高压直流供电和暖通控制等技术，将能源效率(PUE)指标控制在 1.3 以下，比传统风冷数据中心节能 30%以上，电源效率超 90%。

5 服务验收要求

5.1 技术路线和分区要求

建成同时支持 X86 与 ARM 技术路线的三种不同网络环境的业务区，即：政务外网区、互联网区、行业专网业务区。

5.2 满足国产化建设要求

1、政务外网区物理服务器扩容和替换须采用符合国家信创要求的产品；

云服务器须提供符合国家信创要求的操作系统。

2、如国家或省级信创产品采购认定技术标准出台，相关产品需配合完成认定申报。

5.3 满足网络要求

每个云区保证提供政务外网至政务服务区互联服务 2 条（2*10G 专线），技术要求如下：

1、互联专线服务：提供专线 2 条，每条速率 10G、接口为万兆光口，传输延时各云区之间通信延时小于 2 毫秒；

2、误码率≤1e-9；

3、链路延时≤30ms；

4、封包成功率≥99.99%；

每条电路具备双路由环保护。

5.4 满足重大应用容灾能力要求（按需）

1、支持应用双活部署，支持统一云资源管理和全业务容灾能力；

2、支持全量和增量数据同步能力；

3、主备机房网络延时不超过 1.5ms，主备之间通过 2 根及以上的传输专线互联，光缆全程分离路由；

4、提供统一容灾管理中心，提供租户化的容灾计划、容灾监控和故障恢复能力。

5、满足具备异地备份能力，包括支持周期性备份、备份多版本保存、数据恢复、支持对云主机快照全量或增量备份和恢复，支持云数据库物理备份和恢复、支持物理备份，支持全量备份和增量备份等能力。

5.5 满足云平台（云区）安全要求

1、云平台（云区）安全防护系统应支持软件化部署，具有高可用设计和弹性扩展能力；

2、云平台（云区）安全防护系统应能够实现与云平台（云区）联动，用户业务上线后即自动提供安全保障服务；

3、云平台（云区）应提供基础的安全审计功能，支持的审计内容包括但不限于网络设备日志审计、用户行为审计、数据库审计、运维审计等，日志保存时间不低于 6 个月；

4、如国家或省级信息系统关键性基础设施认定标准出台，需配合完成认定申报。

5.6 云平台终验要求

1、平台应具备网络安全技术防护能力及管理能力，符合国家安全政策法规，服务期内须通过三级等级保护测评，并提供第三方测评公司的测评通过报告，须通过国家密码应用安全性测评；

2、自提供服务之日起视上级监管要求一年内通过国家云计算服务安全评估，并在中央网信办网站可查阅。

6 运营及服务要求

6.1 云平台运维要求

云服务商应成立备云平台专业运维服务团队，包含云服务商自有团队、原厂（授权）技术服务团队、安全厂商团队，负责云平台的整体运维。云平台专业运维服务团队至少由云服务商（不少于 3 人）、原厂（授权）技术服务商（不少于 2 人）、安全厂商（不少于 1 人）组成。

运维服务内容包括资源管理、日常监控、故障处理、安全管理、运行分析。根据服务对象不同，可分为平台侧运维服务要求和租户侧运维服务要求。平台侧运维服务包含平台日常运维、容灾和管理等服务。

6.2 日常运行监测要求

云服务商应提供 7*24 小时的监控、值班值守和服务台热线。服务台作为事件管理平台的入口，及时响应云平台用户的各类请求，根据事件的具体情况负责事件的登记、升级、跟踪直至关闭。

按照监控要求和规范，负责执行 7*24 小时监控服务，包括邮件、电话等告警服务。

7*24 小时监控内容包括服务器、存储、网络、云平台、虚拟机，虚拟机的监控服务基于用户自愿的原则。

7*24 小时值班值守服务，加强巡查监测，遇到故障等突发事件，必须立即启动应急响应。

6.3 平台故障处置要求

根据故障的严重程度和影响业务程度的不同，故障级别由高到低分为一级故障、二级故障和三级故障。

一级故障：主要指设备在切换中出现系统瘫痪或业务服务中断，导致设备的基本功能不能实现或全面退化的故障；或在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化；业务不能提供正常服务并有大量用户报障。

二级故障： 主要指设备在切换中出现的影响服务的情况，导致系统性能或服务部分退化的故障；断续或间接地影响系统功能，业务部分功能失效，少量用户报障。

三级故障：设备故障或隐患，暂不影响业务的正常提供。

故障处理过程中做好故障现象和故障处理情况的记录，故障恢复后根据故障的级别和复杂程度在 48 小时内提交故障分析专题报告（一级故障在故障发生的 24 小时内提交，二、三级故障在 48 小时内提交),分析内容包括故障现象、故障类型、故障起始时间、响应时间、修复时间、故障原因、故障处理情况及结果、故障处理人及今后的预防措施等。

7 服务质量考核考评体系

7.1 运维考核

运维考核包含三方面内容：驻场服务考核、月度考核、工单考核。

7.1.1 驻场服务考核

驻场服务地点为衢州市云计算中心，服务商应做好驻场人员的日

常考勤管理。服务商应提供内容真实的《衢州市云计算平台驻场人员运维周报》和《考勤记录》，做为专家评分依据。专家根据运维周报和考勤记录的实际情况，视情评分 0-10 分。

7.1.2 月度考核

7.1.2.1 每月巡检报告

服务商每月对云计算平台进行现场巡检，填写《衢州市云计算平台现场巡检记录表》,每月定期送采购单位备案,作为专家评分依据。

7.1.2.2 每月运维报告

服务商每月 5 日前，向采购单位提交上一个月的《市级单位云资源使用情况》，包括本月整体上云情况，本月新开通、变更、撤销云资源清单、CPU 和内存资源利用率等内容。

7.1.2.3 工单考核

服务商须在 7 日内,按照要求完成经采购单位审批同意的云资源新增、撤销、变更工单。

7.2 平台可用性考核

平台可用性考核包含三方面：平台维护、重大事项保障、应急管理。

7.2.1 平台维护

服务商要提供 7*24 小时的平台维护服务，负责云计算中心内各类系统运行平台的运维服务。服务商须如实填写《衢州市云计算平台故障备案表》，交至采购单位备案，作为专家年度评分依据。

7.2.2 重大事项保障

重大事项保障时间段内，服务商应提供重大事项保障方案、值班表、每日事项记录等相关材料，作为专家年度评分依据。

7.2.3 应急管理

7.2.3.1 应急演练

服务商须制定严谨规范的应急预案，并根据实际工作情况不断完善。服务商根据应急预案，每年至少开展 2 次应急演练。

7.2.3.2 应急事件处理与报告

当云平台（云区）受到攻击或发生其它突发性事故时，服务商须在 1 小时内向采购单位备案，且在 24 小时内恢复正常业务。

服务商应在应急事件发生后 2 个工作日内，向采购单位提交书面报告。

7.3 平台安全性考核

落实政务云平台（云区）安全防护，如出现因政务云平台（云区）安全漏洞造成网络安全事件，按比例扣除云服务费。

7.4 使用单位满意度调查

采购单位每年向市级政务云资源使用单位开展满意度评估。