ICS 35.030
CCS L70

团 体 标 准

T/COSOCC 019—2024

信息技术应用创新 数字政务平台技术要求

Information technology application innovation—Technical requirements of digital government platform

2024－05－31 发布　　2024－05－31 实施

中国基本建设优化研究会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国基本建设优化研究会提出并归口。

本文件起草单位：山东旗帜信息有限公司、国家信息中心、杭州半云科技有限公司、北京易华录信息技术股份有限公司、中电数据服务有限公司、福建捷宇电脑科技有限公司、东软集团股份有限公司、厦门大学、大连倚天软件股份有限公司、北京光梭激光通信科技有限公司、杰创智能科技股份有限公司、山西大众电子信息产业集团有限公司、湖北省楚天云有限公司、成都兴城融晟科技有限公司、讯飞智元信息科技有限公司、山西数字政府建设运营有限公司、北京致远互联软件股份有限公司、北京神州数码云计算有限公司、长河信息股份有限公司、南方电网数字平台科技（广东）有限公司、广东盈世计算机科技有限公司、湖南正宇软件技术开发有限公司、北京启明星辰信息安全技术有限公司、厦门亿联网络技术股份有限公司、北京中超伟业信息安全技术股份有限公司、杭州领信数科信息技术有限公司、北京网御星云信息技术有限公司、航天云网数据研究院（江苏）有限公司、河南明道优术智能技术有限公司、中移（杭州）信息技术有限公司、蓝象标准（北京）科技有限公司、嵩嘉标准化技术服务（北京）有限公司。

本文件主要起草人：邱瀚、王进京、宋小波、秦鹏、何帆、孙高海、刘思瀚、罗晔、侯程、陈细平、谭莹、张立明、陈亮、刘若舒、肖世达、王兴强、陈士星、郑亮、刘股权、回武让、赵宝金、刘江平、邓锐军、刘跃华、王孝军、郭逾、罗远哲、陈淑芬、王斌、吕云云、张浩、李春来、潘悦、刘永进、潘晓东、李帅、王颜颜、张风雷、吴晗、冯大刚、熊凡凡、张德保、王新亮、段小莉、姜冰、张红艳、周紫晗、邱天、乔华阳。

引　言

数字政务的快速演进现已迈入转型关键期，正经历着发展模式的根本转变、应用层次的深化与效益的显著提升。在此过程中，政府功能的转型升级及服务型政府构建，对数字政务提出了更高层次的挑战与要求。以信息技术应用创新为先锋的新兴信息技术正不断涌现，催生新产业、新应用，从而深刻影响着数字政务的发展环境与条件。

以信息技术应用创新为代表的新兴信息技术正催生新的产业与应用模式，进而深刻改变了数字政务的技术生态和基础条件。通过构筑基于信息技术应用创新的数字政务平台，有望最大化地挖掘和利用现有资源，激发新兴信息技术的巨大潜力，推进数字政务的创新发展，增强服务支持能力和安全保障能力，减少不必要的重复建设，并且有效避免各部门之间信息共享不畅所导致的信息孤岛。

T/COSOCC 019《信息技术应用创新 数字政务平台技术要求》与T/COSOCC 020《信息技术应用创新 数字政务平台安全要求》在综合考量计算资源、存储资源、网络资源、信息资源、应用支撑与信息安全等关键要素的基础上，分别从技术和安全角度提出了信息技术应用创新数字政务平台的要求。其中T/COSOCC 019规定了数字政务平台的资源技术要求、应用技术要求、信创硬件系统技术要求、信创软件系统技术要求和信创云系统技术要求；T/COSOCC 020规定了数字政务平台的基础安全、应用安全、服务安全以及安全审计、安全监测要求、安全运维要求和安全管理等要求。

本文件的制定明确数字政务平台技术方面的建设、运营、服务及管理机制，并进一步完善信创环境下的管理策略，以保障数字政务平台的高质量持续发展。本文件详细界定数字政务平台资源技术要求、应用技术要求、信创硬件系统技术要求、信创软件系统技术要求、信创云系统技术要求等多个内容，为各地区在开展信息技术应用创新基础上的数字政务平台的顶层设计、构建实施、应用服务以及运行保障等方面提供指导与规范，以推动数字政务建设迈向高水平、高质量的可持续发展。

信息技术应用创新 数字政务平台技术要求

1 范围

本文件规定了数字政务平台的资源、应用、信创硬件系统、信创软件系统和信创云系统等技术要求。

本文件适用于数字政务平台的规划、建设、管理等活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 9254.2 信息技术设备、多媒体设备和接收机 电磁兼容 第2部分：抗扰度要求

GB/T 15934 电器附件 电线组件和互连电线组件

GB 17625.1 电磁兼容 限值 第1部分：谐波电流发射限值（设备每相输入电流≤16A）

GB 18030 信息技术 中文编码字符集

GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 33476.3 党政机关电子公文格式规范 第3部分：实施指南

GB/T 36441 硬件产品与操作系统兼容性规范

GB/T 36904 电子证照 标识规范

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38664.2 信息技术 大数据 政务数据开放共享 第2部分：基本要求

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

T/COSOCC 011 信息技术应用创新 云计算基础设施即服务（IaaS）通用技术要求

RFC 4627 JavaScript 对象表示法（JSON）的应用程序/JSON媒体类型 （The application/JSON Media Type for JavaScript Object Notation (JSON)）

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字政务平台 digital government platform

数字政府为推动政务治理高效化、便捷化、流程化和模式化，利用数字技术所构建，通过数据共享和业务协同，融合了政务服务过程中的多个业务系统或功能，提供在线服务、信息公开、互动交流、数据共享、智能决策、电子证照等服务，用以推动政府现代化治理和社会进步的数字化、智能化平台。

3.2

资源池 resource pool

一组物理资源或一组虚拟资源的集合，可以从池中获取资源，也可将资源回收到池中。

注：资源包括物理机、虚拟机、虚拟网络设备、物理网络设备和 IP 地址等。

3.3

电子证照 electronic license and certificate

政府部门或相关机构通过数字化技术，将各类证照、证明、许可等官方文件的内容和信息转化为电子形式，并以数字化的方式进行存储、传输和管理。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表(Access Control Lists)
API：应用程序接口（Application Programming Interface）
CPU：中央处理器（Central Processing Unit）
GPU：图形处理器（Graphics Processing Unit）
IOPS：每秒输入/输出读写次数（Input/Output Operations Per Second）
IP: 网际互连协议（Internet Protocol）
IPv6：互联网协议第6版（Internet Protocol Version 6）
JSON： JS对象简谱（JavaScript Object Notation）
NAT：网络地址转换（Network Address Translation）
PCIE：外设部件互连标准（Peripheral Component Interconnect Express）
RAID：独立磁盘冗余阵列（Redundant Array of Independent Disks）
VPC：虚拟专用云（Virtual Private Cloud）
VPN：虚拟专用网络（Virtual Private Network）
XML：可扩展标记语言（Extensible Markup Language)

5 总体框架

数字政务平台技术要求总体框架包括五个部分：数字政务平台资源技术要求、数字政务平台应用技术要求、数字政务平台信创硬件系统技术要求、数字政务平台信创软件系统技术要求和数字政务平台信创云系统技术要求，具体内容详见图1。数字政务平台的软硬件搭建首先应符合国产化要求。

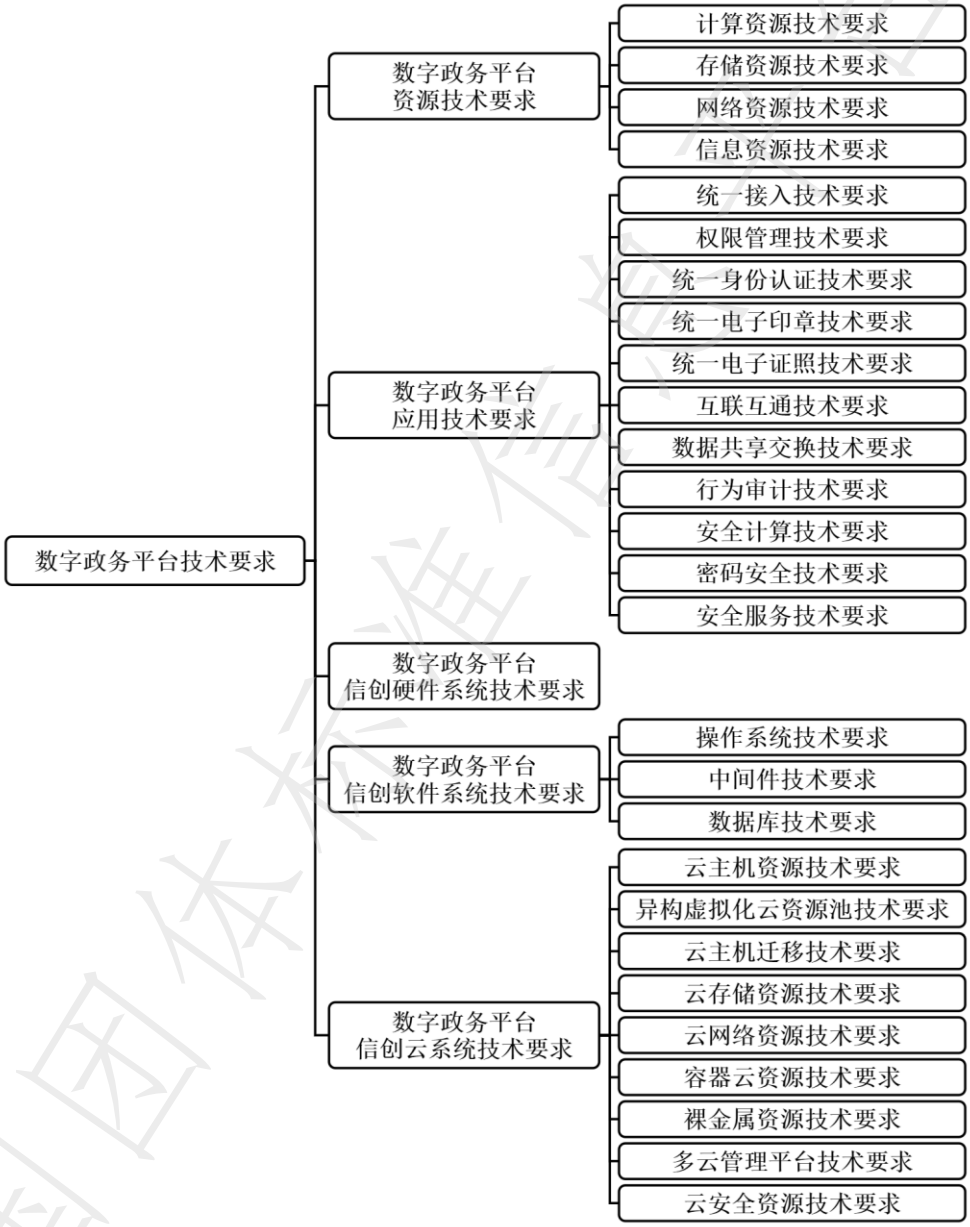

图1　数字政务平台技术要求总体框架

6　数字政务平台资源技术要求

6.1　计算资源技术要求

数字政务平台计算资源应符合下列要求：

a)　支持系统映像添加虚拟机，每台从部署到交付运行的时间应小于 20 min；

b)　支持光盘映像添加虚拟机，每台从部署到交付运行的时间应小于 1 h；

c)　支持释放虚拟机所使用的计算资源、资源重建和删除虚拟机，并保持虚拟机的配置不变；

d) 对主机计算资源进行实时监测，应设置符合经济效益的合理监测阈值，当超过计算资源监测阈值时，应考虑增加计算资源。

6.2 存储资源技术要求

数字政务平台存储资源应符合下列要求：

a) 对于集中式存储环境，多种数据块大小混合读写（顺序、随机、混合）的情况下，存储系统的IOPS（输入/输出操作每秒次数）不小于10万次，读写带宽不低于10 Gb/s，平均响应时间不超过30ms；
b) 对于分布式存储环境，存储系统的多节点并行恢复数据不低于1Tb/h，容量和性能随节点增加而线性增长，如24个节点存储系统每秒操作数不少于300万次，平均响应时间不大于3ms，每节点扩容时间不超过1min；
c) 支持多种形式的存储资源虚拟化，支持多种存储协议融合，支持多种类型端口及协议，支持不同存储介质之间实现双向动态迁移；
d) 具备数据快照、恢复、备份、复制、镜像、克隆、冗余、加密和签名等数据保护功能；
e) 对存储系统资源进行实时监测，应设置符合经济效益的合理监测阈值，当超过存储资源监测阈值时，应考虑增加存储资源。

6.3 网络资源技术要求

数字政务平台网络资源应符合下列要求：

a) 网络层支持云计算技术的资源池动态调度，支持核心交换机虚拟集群技术、接入交换机堆叠技术，支持核心交换机和接入交换机之间的链路捆绑，保证设备和链路冗余；
b) 支持根据组织机构动态分配VPN服务接入数字政务平台网络，并对VPN服务进行监管；
c) 外部接入网络带宽速率应达到千兆链路带宽，内部网络带宽速率应达到千兆链路带宽或万兆以上；
d) 内部网络最大端到端延迟时间应小于100ms，内部网络丢包率应小于0.5‰，防火墙吞吐量不低于100Gb/s，交换机交换容量不低于16Tb/s，交换机包转发率不低于9600Mpps；
e) 出口链路带宽应进行实时监测，若实际监测值超过链路带宽的75%，应考虑扩容。

6.4 信息资源技术要求

数字政务平台信息资源符合下列要求：

a) 应支持信息资源的集中式部署和分布式部署，支持主流国产化数据库的适配，可实现不同业务系统间的数据交换（包括文件型数据和关系型数据），支持主流公文类型、二进制等格式文件的适配；
b) 支持多种类型数据之间的融合、叠加等，并提供二次开发接口；支持融合后的数据服务发布、取消、撤回、删除等功能；
c) 数据交换服务适配器运行环境一次至少加载100个适配器实例，每次至少支持2000条记录交换和20M以内的公文交换；
d) 数据交换服务适配器运行环境应至少支持50个并发数据交换服务，数据交换服务最少支持500个并发数据交换；
e) 交换监控的日志查询响应时间应不超过 3s，交换服务、适配器运行环境的运行状态响应时间不超过15s。

7 数字政务平台应用技术要求

7.1 统一接入技术要求

数字政务平台统一接入技术应符合下列要求：

a) 接入接口应支持XML和JSON数据格式要求，XML格式应符合XML1.0要求，JSON格式应符合RFC 4627要求；
b) 支持主流计算机编程语言，如JAVA、Python、C++、C#等；

c) 接入接口应支持软件开发工具包（SDK）或 API 模式，支持万维网应用程序（Web Service）、表述性状态传递（Restful）两种接口风格，并提供详细的接口技术文档；
d) 业务应用系统应兼容超文本 5.0（HTML5）标准规范的浏览器，移动端 APP 程序支持国产化操作系统。

7.2 权限管理技术要求

数字政务平台权限管理技术应符合下列要求：
a) 支持根据用户登录名称获取该用户具有访问权限的应用列表或功能列表；
b) 支持根据用户登录名称和应用标识，验证该用户是否具有此应用或功能的访问权限；
c) 支持基于 ACL、基于角色的访问控制（RBAC）等多种方式实现权限控制，权限控制颗粒度应到每一个功能点；
d) 支持基于角色、菜单实现用户菜单级的授权管理，菜单权限可自由分配；
e) 支持根据业务需求，对业务数据进行分级分类管理，对业务数据权限进行控制。

7.3 统一身份认证技术要求

7.3.1 用户管理技术要求

数字政务平台用户管理技术符合下列要求：
a) 应支持以实名制为基础，对用户信息进行整合，构建完整、统一、可信的用户资源信息库，可根据应用需要进行数据同步，支持用户集中管理和分级管理模式；
b) 应支持用户凭证信息生命周期的管理，及凭证的创建、注销、修改、删除等操作；
c) 应支持用户分组管理模式，可基于组织机构或角色对用户进行分组管理；
d) 应按照管理、操作、审计三权分立的设计原则，针对不同的管理要求设立相应的平台管理员、应用系统管理员和安全审计员三类管理角色。

7.3.2 认证管理技术要求

数字政务平台认证管理技术符合下列要求：
a) 应支持多种登录认证方式，及高级别认证方式向下兼容低级别认证方式；
b) 应支持根据数字政务平台的不同安全需求，制定不同的认证等级策略，如提供认证安全等级向下兼容策略；
c) 身份认证应支持口令认证、证书认证、令牌认证等认证方式，按照 GB/T 25064 的规定设计数字证书；
d) 系统应具有可扩展性，可实现对动态口令、生物特征信息等其他组合认证方式的支持；
e) 应支持安全认证服务通过认证服务接口，实现对用户身份的统一认证管理。

7.3.3 授权管理技术要求

数字政务平台授权管理技术符合下列要求：
a) 应支持统一的访问控制和权限管理，支持集中授权管理和分级授权管理模式，支持角色组管理机制，实现对用户的分组授权；
b) 应支持按需对数字政务平台的授权进行安全策略配置，支持数字政务平台的粗粒度授权和业务角色级的细粒度授权；
c) 应支持分级授权管理模式，可基于组织机构完成数字政务平台的分级授权管理；
d) 应支持业务操作和安全审计权的分离，确保统一认证管理系统的自身运行安全。

7.3.4 审批管理技术要求

数字政务平台审批管理技术应符合下列要求：
a) 支持对用户基本信息变更、业务应用操作和访问控制授权等行为操作的电子化审批；
b) 支持详细记录每一行为操作的审批记录、审批时间、审批事项及审批人；
c) 支持审批记录结果的分类查询、综合查询、持久化存储和统计分析，并定期形成报告；
d) 关键的审批步骤应支持数字签名，确保责任落实到人的要求。

7.4 统一电子印章技术要求

数字政务平台统一电子印章技术应符合下列要求：

a) 电子印章数据结构应包括待电子签章数据、电子印章所有者数字证书、签名算法标识、签名值、时间戳等信息；
b) 电子印章应用时应验证数据格式、电子签章签名、所有者证书、签章时间、原文杂凑、时间戳等信息的正确性和有效性；
c) 验证比对过程失败时应退出应用流程并返回验证失败原因，电子印章执行更新、重签发等操作导致验证比对失败时，应重新制作电子印章；
d) 签章数据在开放版式文档（OFD）版本文件中使用时，应符合 GB/T 33476.3 的规定。

7.5 统一电子证照技术要求

数字政务平台统一电子证照技术符合下列要求：

a) 应支持根据持证主体和证照类型检索证照；持证主体是自然人时宜使用公民身份号码，是法人或其他组织时宜使用统一社会信用代码；
b) 检索结果中应包含符合 GB/T 36904 规定的电子证照标识；
c) 应支持电子证照获取时获取该证照的多项元数据信息，可请求下载该证照的电子证照原件或加注件，获取证照信息或电子证照文件前应获得持证主体直接或间接的授权；
d) 应支持对给定的证照元数据信息进行核对，支持进行真伪验证及管理状态核对。

7.6 互联互通技术要求

7.6.1 IP 网间互联互通技术要求

数字政务平台IP网间互联互通技术符合下列要求：

a) 外部路由协议宜采用边界网关协议 4.0（BGP-4），内部路由协议宜采用开放最短路径优先（OSPF）或中间系统到中间系统（IS-IS），并提供良好的路由更新性能，能正确而迅速地更新和交换路由；
b) 应提供必要的网络管理功能和运行监控手段，如监测、统计互联链路的流量等；
c) 应支持网络节点的备份和节点之间的线路保护，提供网络安全防范措施，保证网络传输质量。

7.6.2 系统间互联互通技术要求

数字政务平台系统间互联互通技术应符合下列要求：

a) 支持分级分类采集数字政务平台的运行状态数据，并向多级平台自动上报运行状态数据；
b) 支持实时监测运行在数字政务平台上业务应用和服务的运行状况；
c) 支持多个交换平台之间的数据交换，以及最短路径数据交换；
d) 数据交换过程应采用认证机制、授权机制和访问控制措施，应采用加密和完整性保护机制。

7.7 数据共享交换技术要求

数字政务平台数据共享交换技术符合下列要求：

a) 应支持根据数据的重要性、量级、使用频率、存储环境等因素对数据信息资源进行分域分级管理，应预先对每类数据设置访问策略、共享策略和共享范围，未授权条件下禁止数据下载、复制、截屏等操作；
b) 应支持根据业务需求、管理范围、组织架构等设置访问控制策略，应统一设置、统一注销、统一鉴别、统一授权、集中鉴权、集中审计，对特定数据的访问主体进行实时授权或取消授权；
c) 敏感数据应设置双活或多活存储机制，宜采用分布式存储，存储信息应符合 GB/T 38664.2 和 GB/T 39477 的要求，防止信息通过关联分析等技术手段被恢复，并建立数据冗余一致性校验策略；
d) 共享交换过程中应使用数字证书、密码标识、生物特征、交叉认证等技术实现身份鉴别，采用两种或两种以上的鉴别技术对数据访问主体进行身份鉴别；

e) 应具备监控数据共享传输过程和过程追溯的能力，支持在数据共享不完整时清除传输缓存数据，共享完成后清除传输历史缓存数据，跟踪和记录数据共享过程，发现问题时及时告警并进行阻断；
f) 应支持定义空值、内容冲突、不合规约束等数据质量评价条件，检验并评价数据共享交换后的数据质量；
g) 应支持数据逻辑存储，满足不同数据类型、容量和使用的逻辑存储管理，严格限制批量修改、拷贝、下载等操作的权限，建立数据血缘关系梳理。

7.8 行为审计技术要求

数字政务平台行为审计技术应符合下列要求：
a) 支持在事前控制、过程监督、事后追溯和闭环整改的机制下记录、分析和检查用户行为和系统状况，判断其是否符合预定的安全策略；
b) 支持通过分析和检查发现系统存在的安全漏洞、潜在的安全威胁，并对可能造成的后果进行分析和评估，根据审查结论进行整改；
c) 支持实时对业务审批操作、系统管理操作、用户操作等行为进行记录，记录内容包括但不限于：登录 IP 地址、登录用户标识、行为分类、动作名称、操作系统名称、操作对象、操作结果等信息；
d) 支持定期审计行为记录内容，并形成数字政务平台行为审计报告。

7.9 安全计算技术要求

数字政务平台安全计算技术应符合下列要求：
a) 支持硬件隔离机制，与不可信环境实现硬件隔离，硬件资源应隔离为安全资源和普通资源；
b) 支持可信应用间的调用执行、可信应用之间的隔离，支持可信验证机制，具备多线程、多进程等计算能力；
c) 支持对安全计算内核和应用合法性的本地或远程验证，提供对通信通道传输数据的保密性保护和完整性保护；
d) 支持对物理节点、服务调用、密钥操作、数据操作进行访问控制规则的安全策略配置；
e) 支持通过监控分析发现异常问题，制定异常处置规则，快速修复异常并及时上报。

7.10 密码安全技术要求

密码安全技术应用应符合下列要求：
a) 使用的密码算法、密码技术应符合法律、法规的规定和密码相关国家标准的有关要求；
b) 使用的密码产品、密码服务应通过国家密码管理主管部门核准、许可；
c) 使用的密码产品，应符合 GB/T 37092 中二级及以上的安全要求；
d) 密码模块应提供基于角色、基于身份的鉴别机制，提供口令、PIN、秘钥、令牌、生物特征等多种类型的鉴别方式；
e) 具备相关密钥管理优化机制，确保传输安全与数据安全。

7.11 安全服务技术要求

安全服务应符合下列要求：
a) 支持按最小化原则关闭不必要的服务和端口，禁止特权账号和功能，严格分配文件权限，开启基础访问控制和强访问控制，并记录用户访问信息；
b) 支持部署轻量级的防病毒引擎，确保全网一致的防病毒策略和实时查杀能力，提供恶意代码检测和处置服务，支持删除、修复、隔离感染文件；
c) 提供安全基线检查，扫描系统服务，检查用户账号是否存在问题，对操作系统配置项进行检查和设置；
d) 支持安全审计记录关键事件的日期、时间、用户、事件类型、是否成功等信息，保护审计记录，定期备份，防止非授权的删除或修改，对授权的删除、修改等行为在操作前应进行提示。

8 数字政务平台信创硬件系统技术要求

数字政务平台信创硬件系统技术要求见表1。

表1　信创硬件系统技术要求

类别	内容	要求
硬件	CPU	应支持2种及以上的国产CPU，服务器核心数量不小于16核，主频不低于2.0GHz，支持硬件虚拟化。
	内存	双通道，内存频率不低于2666 MHz，内容容量不小于32GB。
	存储接口	SATA 3.0 接口数不小于2个； M.2 接口数不小于1个，支持非易失性内存主机控制器接口规范（NVME）协议。
	显卡插槽(不含一体机)	标准PCIE显卡插槽数不低于1个，位宽在x8及以上。
	其他接口	USB接口数不小于4个；VGA接口数不小于1个；HDMI接口数不小于1个； 千兆RJ45网口数不小于2个；音频接口数不低于1组。
	扩展插槽(不含一体机)	PCIE3.0x16扩展插槽数不小于2个； PCIE3.0x8扩展插槽数不小于5个。
电磁兼容性	无线电骚扰	应符合GB/T 9254.2的规定，在产品出厂文件中应标明选用的是A级或B级所规定的无线电骚扰限值。
	谐波电流	应符合GB 17625.1中对D类限值的要求。
	抗扰度	应符合GB/T 9254.2的规定。
电池及电源	电池保护	电池应具有过充电保护、过放电保护、过流保护、短路保护、过温保护，在过充电、过放电、过流，短路和过温状态下，电池不应出现爆炸、起火、冒烟或者漏液等状况。短路保护瞬时充电后，电池电压应不小于标称电压。
	电池循环寿命	产品电池的充放电循环次数应不小于500次。循环次数指当连续3次放电容量低于其标称容量的75%时记录的充放电次数。
	电源适应能力	对于交流供电的产品，应能在220V±22V，50Hz±1Hz条件下正常工作； 对直流供电的产品，应能在直流电压标称值的(100±5）%的条件下正常工作；标称值应在产品标准中规定，对于电源有特殊要求的单元应在产品标准中加以说明； 电线组件应符合GB/T 15934的规定。

9　数字政务平台信创软件系统技术要求

9.1　操作系统技术要求

操作系统应符合GB/T 36441及下列要求：

a)　操作系统应兼容主流的国产硬件平台，支持 2 种及以上的国产 CPU；
b)　内置高级安全特性，如防病毒、防火墙、入侵检测和防御系统等，支持安全启动和数据加密；
c)　支持操作系统国产化产品适配认证，验证其在信创环境下的功能、性能、安全性，能与其他系统和平台进行有效的数据交换和协同工作，支持开放标准和协议；
d)　支持多种中文输入法，应符合 GB 18030 的规定，提供图形化软件包升级工具，支持远程和本地在线升级；
e)　支持主流软件应用，确保现有的软件生态可以平稳迁移到国产操作系统上；
f)　支持安全可靠芯片，包括可信密码模块（TCM）、可信平台控制模块（TPCM）和可信平台模块 2.0 版本（TPM2.0）及其服务器整机。

9.2　中间件技术要求

9.2.1 消息中间件技术要求

消息中间件应符合下列要求：

a)　支持 2 种以上的国产软硬件环境，如 32 和 64 位的 X86、ARM 平台下运行；
b)　支持多种通讯链路和网络环境方式且支持动态增加应用节点；
c)　支持本地存储和分布式存储，具备集群和负载均衡功能；
d)　支持自定义消息队列、自定义队列字节长度和自定义队列溢出行为方式；

e） 支持配置文件和传输数据的自动加解密处理，支持加密算法位数配置；
f） 支持第三方安全接口，如消息安全、链路安全、节点安全、配置安全、身份认证、访问控制、操作安全等。

9.2.2 应用服务器中间件技术要求

应用服务器中间件应符合下列要求：
a） 支持 2 种以上的国产软硬件环境，支持多种主流国产数据库系统；
b） 支持多种编程语言和开发框架，提供中文主控界面，符合国家标准字符集 GB 18030 的规定。

9.3 数据库技术要求

数据库应符合下列要求：
a） 支持安全标记的强制访问控制，支持国产加密算法，支持 2 种以上的国产软硬件环境；
b） 具备身份鉴别、自主访问控制、数据流控制、安全审计、数据完整性、数据保密性、可信路径、推理控制等功能；
c） 列存储功能支持分段式压缩技术和常用的压缩算法，列式表支持粗粒度智能索引；
d） 支持读写分离和分布式存储，具备可视化操作、自动化运维和管理功能；
e） 支持数据库国产化产品适配认证，验证信创环境下的功能、性能、安全性。

10 数字政务平台信创云系统技术要求

10.1 云主机资源技术要求

云主机资源符合下列要求：
a） 物理主机 CPU 芯片和物理主机操作系统均应采用国产化芯片，支持在不同可用区（AZ）中创建 X86、ARM 或其他单字长定点指令平均执行速度（MIPS）物理主机的云主机；
b） 使用 X86、ARM 主机时支持国产化 GPU，可透传或虚拟 GPU，主机包括国产化 CPU；
c） 可调整 CPU、内存、磁盘等配置，实现跨主机迁移和全生命周期管理；
d） 创建云主机时可自动分配或指定 IP 地址，配置多块辅助网卡及安全组；
e） 应支持回收站恢复云主机和设置回收站保存时间，支持云主机亲和性或反亲和性调度；
f） 应支持计算能力弹性伸缩和 IPv6，同时，系统盘和数据盘支持分布式块存储。

10.2 异构虚拟化云资源池技术要求

异构虚拟化云资源池符合下列要求：
a） 一套云平台应支持同时管理不同 CPU 架构的计算资源池；
b） 云平台应支持选择不同资源池创建不同 CPU 架构的云主机；
c） 信创云应支持按照不同 CPU 架构扩容计算节点服务器；
d） 应支持计算节点和控制节点的动态扩容；
e） 同 CPU 架构的云主机可部署在同一个虚拟子网中。

10.3 云主机迁移技术要求

云主机迁移应符合下列要求：
a） 支持在同一个计算资源池中部署不同 CPU 架构的两种或多种物理主机；
b） 支持云主机在同一个计算资源池的相同 CPU 架构不同品牌物理主机之间迁移。

10.4 云存储资源技术要求

云存储资源应符合下列要求：
a） 支持集中式或分布式架构云存储，支持块存储、对象存储、文件存储，支持高可用部署方式和弹性扩容，支持对象分块上传和数据迁移工具；
b） 支持多副本或冗余校验存储机制，支持监控集群容量、健康状态、服务性能等；
c） 支持管理云硬盘全生命周期，创建、挂载、卸载、扩容、快照、属性修改、标签、分配至租户；
d） 控制台应支持创建、删除、回滚快照，配置自动快照策略，支持从快照创建云硬盘；

e) 支持自动设置云硬盘容量对 IOPS、带宽的限速，支持云硬盘回收站，误删后恢复，批量操作；
f) 具备严格访问授权机制，支持安全套接层（SSL）加密传输，提供多种安全配置、ACL 控制和防盗链功能。

10.5 云网络资源技术要求

云网络资源符合下列要求：
a) 应具备软件定义网络框架，实现网络的可编程，方便用户获得灵活的网络控制；
b) 应支持基于虚拟局域网（Vlan）或虚拟可扩展局域网（VxLAN）技术的云主机互通，实现多功能网络使用场景；
c) 应支持多种网关，如服务器负载均衡（SLB）、NAT、VPN；以及网络配置，如动态主机配置协议（DHCP）、ACL、路由表；
d) 应支持 IPv6，弹性 IP 带宽限速，负载均衡器支持 IPv6 地址绑定、跨 AZ 集群部署和会话同步；
e) 应实时监控弹性 IP、NAT 网关性能、负载均衡器性能指标，设置报警策略；
f) VPC 内云主机和物理主机可共享 NAT 网关，支持 VPC 互联，VPC 支持子网划分，分布式路由功能，自定义地址池和安全组。

10.6 容器云资源技术要求

容器云资源应符合下列要求：
a) 托管集群监控支持日志中心，日志对接内嵌式存储系统（ES）、kafka 等系统，支持实时监控集群、节点、置标语言（POD）、负载均衡性能，自定义告警规则和通知；
b) 支持基于 CPU、内存等指标的节点弹性伸缩，定时周期策略伸缩；
c) 多云容器平台支持通过集群联邦纳管已有集群，实现统一管理，支持私有、公有镜像仓库，第三方仓库拉取镜像，跨 Region 镜像同步；
d) 支持 Helm、Kubetpl、Spinnake、Octant 等模板管理，部署和管理应用实例；
e) 支持应用重启、停止、启动、删除，有/无状态部署，短时任务等操作；
f) 支持不同类型的 Kubernetes Service 发布，集群内外访问；
g) 支持 ConfigMap 和 Secret 配置项，保存应用配置参数和敏感信息；具备 Prometheus 自定义指标接入，关联分析、指标聚合功能。

10.7 裸金属资源技术要求

裸金属资源应符合下列要求：
a) 支持全生命周期管理，包括创建、删除、启动、关闭、重装系统等；
b) 硬盘 RAID 配置支持多种 RAID 级别和文件系统挂载点；
c) 支持自定义镜像和批量创建裸金属服务器；
d) 支持网络管理、安全组设置，及 VPC 互联；
e) 支持裸金属与云主机通信，具备 NAT、专线、VPN、负载均衡等功能。

10.8 多云管理平台技术要求

多云管理平台应符合下列要求：
a) 统一多云资源管理，支持多个信创云平台、数据中心的资源统一视图和管理，包括虚拟资源、云主机、云存储和云网络；
b) 统一用户管理，对接各信创云平台的用户体系，实现统一用户的生命周期管理；
c) 统一运维管理，支持对多个信创云平台的物理主机和云主机的日常运维工作，包括文件操作、指令记录、运维策略等；
d) 统一监控管理，对多个信创云平台的物理主机和云主机进行统一监控和告警设置；
e) 支持平台容错及高可用管理，支持高可用部署、容器化部署，并能自动恢复异常；
f) 支持平台安全管理，使用 SM3 或 SM4 算法进行加密，支持国密 HTTPS 和国密 CA 证书。

10.9 云安全资源技术要求

云安全资源应符合下列要求：

a) 支持以实名制为基础，确保用户身份标识唯一性，支持多种身份鉴别措施，如密码、短信验证、Ukey 等，提供统一用户和权限管理，限制管理员访问权限；
b) 加固物理主机安全、收缩网络暴露面，支持弹性云防护，建设统一安全接入边界；
c) 隔离虚拟资源，实现物理主机与云主机隔离，并加固云主机操作系统安全；
d) 具备实现云租户隔离，自定义网络和访问控制，支持 API 身份验证和加密传输；
e) 具备统一管理平台，支持全生命周期管理，实现安全审计和智能分析，发现并处理安全问题。

参考文献

[1] GB/T 21063.2 政务信息资源目录体系 第2部分：技术要求
[2] GB/Z 24294.3 信息安全技术 基于互联网电子政务信息安全实施指南 第3部分：身份认证与授权管理
[3] GB/T 33780.1 基于云计算的电子政务公共平台技术规范 第1部分：系统架构
[4] GB/T 36905 电子证照 文件技术要求
[5] GB/T 39044 政务服务平台接入规范
[6] GB/T 39554.1 全国一体化政务服务平台 政务服务事项基本目录及实施清单 第1部分：编码要求
[7] DB23/T 2843 政务信息资源体系总体架构
[8] DB37/T 4630.2 电子政务外网 第2部分：网络接入要求
[9] DB43/T 2254 信息技术应用创新工程建设规范 第15部分：云计算通用技术要求
[10] DB52/T 1619 电子政务外网与业务网融合规范