

数 字 山 东 工 程 标 准

SZSD 0023—2024

政务云平台供应链管理规范

Government Cloud Platform Supply Chain Management

2024 - 04 - 15 发布

2024 - 06 - 01 实施

目 次

前 言	2
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 供应链 supply chain	1
3.2 需方 acquirer	1
3.3 供方 supplier	1
3.4 供应关系 supplier relation	1
3.5 政务云平台供应链 government cloud platform supply chain	1
4 政务云供应链管理目标	2
5 管理要求	2
5.1 组织管理	2
5.1.1 机构管理	2
5.1.2 制度管理	2
5.1.3 人员管理	2
5.1.4 供应商管理	3
5.1.5 知识产权管理	3
5.2 活动管理	3
5.2.1 采购管理	3
5.2.2 过程管理	3
5.2.3 运维管理	4
5.2.4 废止管理	4
5.3 安全管理	4
5.3.1 物理环境	4
5.3.2 访问控制	4
5.3.3 风险控制	4
5.3.4 应急安全	5
参 考 文 献	6

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。

本文件由山东省大数据局提出、归口并组织实施。

本文件起草单位：山东省大数据局、山东省大数据中心、北京阿斯科科技有限公司、道普信息技术有限公司、北京明洋科技有限公司。

本文件主要起草人：魏淑斌、张荣光、崔秋红、杨娜、张林、李波、贾风钊。

政务云平台供应链管理规范

1 范围

本文件给出了政务云平台供应链管理目标，规定了政务云平台供应链组织管理、活动管理和安全管理的要求。

本文件适用于指导政务云平台供应链中的供方开展供应链组织管理、活动管理和安全管理工作，可为云服务商自查或第三方机构开展政务云平台供应链安全风险评估提供依据，也可作为政务云平台主管监管部门提供参考。

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 25069—2022 信息安全技术 术语

GB/T 36637—2018 信息安全技术 ICT 供应链安全风险管理指南

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

GB/T 25069—2022、GB/T 36637—2018 和 GB/T 39204—2022 中界定的以及下列术语和定义适用于本文件。

3.1 供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

3.2 需方 acquirer

从其他组织获取产品或服务的组织或个人。

3.3 供方 supplier

提供产品或服务的组织或个人。

3.4 供应关系 supplier relation

需方和供方之间的协议，可用于开展业务、提供产品或服务。

3.5 政务云平台供应链 government cloud platform supply chain

政务云平台供应链，是指为满足供应关系通过资源和过程将需方（政务云平台主管部门）、供方（政

务云平台服务商)连接的网链结构,包含受政务云平台服务商雇佣或委托,支持、承担供应链需求的供应商、次级供应商及产品和服务供应商。

4 政务云供应链管理目标

- a) 供应链完整性:保障在政务云供应链所有环节中,产品和服务及其所包含的组件、部件、元器件、数据等不被植入、篡改、替换和伪造。
- b) 供应链保密性:保障供应链上传递的信息不被泄露给未授权者。
- c) 供应链可用性:保障需方对供应链的使用。一方面,确保供应链按照与需方签订的协议能够正常供应,不易被人为或自然因素中断,即可供应性;另一方面,即使在供应链部分失效时,仍能保持连续供应且快速恢复到正常供应状态的能力,即弹性。
- d) 供应链可控性:保障需方对产品和服务或供应链的控制能力。可控性包括:供应链可追溯性,即一旦发生供应链安全问题,可以有效识别出现问题的环节、供应商和组件,并可进行追溯或修复;可控性,也包括需方对供应链信息的理解或透明度、用户对自己数据的支配能力、用户对自己所拥有和使用产品的控制能力、用户对使用产品和服务的选择权和产品和服务的行为与合同协议相符等。

5 管理要求

5.1 组织管理

5.1.1 机构管理

机构管理要求主要包括:

- a) 明确政务云供应链安全管理机构或团队,指定政务云供应链安全管理负责人,明确其应满足的相关任职资格和职责分工,同时向需方公开报送政务云供应链安全管理负责人及联系方式;
- b) 提供用于政务云供应链安全管理的资金、人员和权限等可用资源。

5.1.2 制度管理

制度管理要求主要包括:

- a) 制定政务云供应链安全管理的总体方针,说明供应链安全管理的总体目标、范围、原则和安全框架等;
- b) 建立政务云供应链安全管理策略,包括但不限于风险管理策略、供应方选择和管理策略、产品开发采购策略、安全维护策略;
- c) 建立政务云供应链安全管理制度,包含供应链生命周期中的主要活动和外部供应商管理等内容;
- d) 定期或在发生重大安全事件、外部环境重大变化、组织策略变化时,对政务云供应链安全管理制度(含自身和供应商制度、流程、规范、应急预案等的执行和演练情况)进行检查和审定,对存在不足或需要改进的安全管理制度进行修订。

5.1.3 人员管理

人员管理要求主要包括:

- a) 制定政务云服务人员的安全要求,包括云服务管理者、实施人员和供应商人员;
- b) 制定政务云服务人员的操作规范,如设备上架替换、产品更新升级、运行维护、信息保密、第三方设备接入等操作;

- c) 对供应商人员进行背景审查，或要求供应商提供可信的人员背景审查结果；
- d) 与授权访问政务云基础设施的服务人员签订安全保密协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等；
- e) 定期开展政务云供应链安全专项培训，对象宜包含所有授权访问政务云基础设施的服务人员。

5.1.4 供应商管理

供应商管理要求主要包括：

- a) 形成供应商清单（含免费、开源产品），并注明哪些产品和服务对政务云的安全存在重要影响；
- b) 建立供应商选择策略和制度，根据产品和服务的重要程度对供应商进行评估，调查其是否曾发生重大供应链安全事件；
- c) 要求供应商对所提供产品和服务的设计、研发、生产、交付等关键环节加强安全管理；
- d) 要求供应商配合开展供应链安全监督和检查；
- e) 明确供应商的安全分工与责任，对其所提供的安全措施合规性进行持续监控和考核。

5.1.5 知识产权管理

知识产权管理要求主要包括：

- a) 要求产品和服务的供应商对产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等知识产权获得10年以上授权，或在网络产品和服务使用期内获得持续授权；
- b) 充分熟悉所使用产品和服务的知识产权，对自主研发软硬件产品的知识产权进行规范管理，防止侵权。

5.2 活动管理

5.2.1 采购管理

采购管理要求主要包括：

- a) 通过采购文件、协议等要求供应商对政务云供应链安全进行承诺，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或者必要的技术支持服务等；
- b) 建立和维护合格政务云供应商目录。应选择有保障的供应商，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险；
- c) 对于严重违法法律法规及供应链安全相关管理要求的供应商应从合格供应商目录中移除；
- d) 强化政务云采购渠道管理,保持采购的产品和服务来源的稳定或多样性；
- e) 采购网络关键设备和网络安全专用产品目录中的设备产品时,应采购通过国家检测认证的设备和产品。

5.2.2 过程管理

过程管理要求主要包括：

- a) 制定和实施防贗品的策略和规程，检测并防止贗品组件进入政务云平台；
- b) 确认所收到的产品或组件真实且未被改动，如光学标签等。对于硬件，应要求供应商提供详细和完整的组件清单和产地清单；
- c) 采用技术措施对产品和服务（包括但不限于产品设计、开发、集成、运维、物流等各阶段）进行安全技术检测（产品组件真实性、后门木马检测、漏洞检查、渗透测试等）；

- d) 针对非成品软件，建立开源及第三方组件的入库和使用审批机制，对来源于开放源代码社区和第三方的代码、组件和软件，进行完整性验证、安全性测试和依赖关系分析，保障开源或第三方组件来源可靠、安全风险可消除或控制，构建形成软件物料清单和软件构成图谱；
- e) 自行或委托第三方网络安全服务机构对定制开发的软件（云服务提供）进行源代码安全检测，出具代码安全检测报告。

5.2.3 运维管理

运维管理要求主要包括：

- a) 要求产品和服务供应商提供中文版运行维护、二次开发等技术资料；
- b) 在产品进行升级维护时，采用安全可控的渠道获取软件升级包、补丁包，并开展相应的安全测试、完整性校验等工作；
- c) 对重要设备进入和离开云物理环境进行授权和监控，并制定和维护相关记录；
- d) 要求软件产品供应商持续跟踪所使用开源和第三方组件的使用状态、安全状态，对于存在安全风险的，应及时通报，并采取更新、修复等措施；
- e) 要求软件产品供应商在发布漏洞补丁前便应通知，且允许对漏洞补丁进行审查、验证、自行安装；
- f) 依据国家有关政策制度、法律法规等要求，定期开展政务云网络安全等级保护测评、商用密码应用安全性评估、网络安全风险评估等安全检查。

5.2.4 废止管理

废止管理要求主要包括：

- a) 建立软硬件产品废止处理规范流程，包括但不限于下架、停用、卸载和数据清除或迁移等内容；
- b) 软硬件产品在终止服务之后，应制定制定服务下线方案与计划，保护隐私安全与数据安全。

5.3 安全管理

5.3.1 物理环境

物理环境要求主要包括：

- a) 确保外部人员访问政务云基础设施受控区域前得到授权或审批，由专人全程陪同，并登记备案；
- b) 定期对政务云基础设施部署的物理环境安全进行检查及评估，预防自然灾害或不可抗力的外因造成供应中断。

5.3.2 访问控制

访问控制要求主要包括：

- a) 按照“必需知道”和“最小授权”原则对供应商相关人员授权，确保只能访问其需要的系统和数据；
- b) 及时终止离岗和调任政务云服务人员对政务云基础设施的访问权限；
- c) 在系统集成商、产品供应商和外部服务提供商发生变更的情况下，更新相关服务人员访问权限等控制措施。

5.3.3 风险控制

风险控制要求主要包括：

- a) 定期对政务云服务人员的访问活动进行审计和监控，及时发现异常行为和潜在风险；

- b) 定期对采购的产品和服务情况进行风险预判分析，重点对关键组件供应链信息（包括但不限于存在安全漏洞、断供、知识产权纠纷、政策法律威胁等）进行研判，并及时处置；
- c) 定期或不定期检查所有授权访问政务云基础设施人员的工具设施，确保不存在恶意程序、漏洞及其他安全缺陷；
- d) 制定有效的数据存储介质管理策略，防止对存储介质的非法授权访问、变更、删除和破坏。

5.3.4 应急安全

应急安全要求主要包括：

- a) 制定政务云供应链安全事件应急处置管理机制，建立统一的供应链安全事件管理台账；
- b) 定期组织政务云服务人员进行应急相关培训和应急演练，并保存相关记录；
- c) 在发生政务云供应链安全事件后，应及时采取相应补救措施，记录事件情况；
- d) 将下游供应商的供应链安全风险和事件及时同步给云服务客户和监管机构。

参 考 文 献

- [1] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求
 - [2] GB/T 31167-2014 信息安全技术 云计算服务安全指南
 - [3] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求
 - [4] GB/T 36637-2018 信息安全技术 ICT 供应链安全风险管理指南
 - [5] GB/T 39276-2020 信息安全技术 网络产品和服务安全通用要求
 - [6] GB/T 32921-2016 信息安全技术 信息技术产品供应方行为安全准则
-