**ICS** 35.040

**L** 80



中华人民共和国国家标准

GB/T XXXXX—XXXX

|  |  |  |
| --- | --- | --- |
|  |  |  |

信息安全技术

信息技术产品供应链安全要求

Information security technology－Security requirements for supply chain of information technology products

|  |
| --- |
|  |
| 在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。 |

XXXX-XX-XX发布

XXXX-XX-XX实施

国家市场监督管理总局

国家标准化管理委员会

发 布

**目 次**

[前  言 III](#_Toc46038966)

[1 范围 1](#_Toc46038967)

[2 规范性引用文件 1](#_Toc46038968)

[3 术语和定义 1](#_Toc46038969)

[4 基本安全要求 2](#_Toc46038975)

[4.1 供应方安全要求 2](#_Toc46038976)

[4.2 需求方安全要求 2](#_Toc46038977)

[参考文献 3](#_Toc46038978)

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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、阿里云计算有限公司、华为技术有限公司、联想（北京）有限公司、中国平安保险（集团）股份有限公司、深信服科技有限公司、国家互联网应急中心、中国网络安全审查技术与认证中心、北京赛西科技发展有限责任公司、北京北信源软件股份有限公司、北京山石网科信息技术有限公司、北京安信天行科技有限公司、阿里巴巴（北京）软件服务有限公司、新华三技术有限公司、国网区块链科技（北京）有限公司、北京天融信科技有限公司。

本文件主要起草人：孙彦、赵波、刘贤刚、张大江、樊洞阳、李汝鑫、赵江、叶润国、朱雪峰、任泽君、钟力、赵晓溢、毛力霞、彭晋、万晓兰、申永波、王博、杨珂、杨剑。

信息安全技术 信息技术产品供应链安全要求

1. 范围

本文件规定了信息技术产品供应方和需求方应满足的供应链基本安全要求。

本文件适用于政务信息系统、关键信息基础设施的信息技术产品供应链安全管理活动，也可为其他信息系统的供应链安全管理活动提供参考。

1. 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 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理指南

1. 术语和定义

GB/T 32921—2016、GB/T 36637—2018界定的以及下列术语和定义适用于本文件。

1.

信息技术产品 information technology product

具有采集、存储、处理、传输、控制、交换、显示数据或信息功能的硬件、软件、系统和服务。

注：本文件中信息技术产品主要包括核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对政务信息系统、关键信息基础设施安全有重要影响的信息技术产品。

[来源：GB/T 32921－2016，定义3.1，有修改]

1.

需求方 acquirer

获取信息技术产品的组织。

注：本文件中需求方主要包括政府部门和关键信息基础设施运营者。

[来源：GB/T 36637－2018，定义3.1，有修改]

1.

供应方 supplier

提供信息技术产品的组织。

注：供应方主要包括信息技术产品供应商、服务提供商、系统集成商、生产商、销售商、代理商等。

[来源：GB/T 36637－2018，定义3.2，有修改]

1.

信息技术产品供应链 information technology product supply chain

通过资源和过程将需求方、供应方相互链接的网链结构，用于将信息技术产品提供给需求方。

[来源：GB/T 36637－2018，定义3.4，有修改]

1. 基本安全要求

4.1 供应方安全要求

供应方应：

1. 声明不会通过在信息技术产品中设置后门，或利用提供产品的便利条件非法获取用户数据、控制和操纵用户系统和设备，不会利用需求方对信息技术产品的依赖性谋取不正当利益，不会出于市场竞争的需要强迫需求方对信息技术产品进行升级或更新换代。
2. 承诺发现信息技术产品存在安全缺陷、漏洞等风险时，立即采取补救措施，包括但不限于漏洞修复、安全替代方案等，并及时通知合作伙伴和需求方。
3. 对信息技术产品研发、制造过程中涉及的外国实体拥有或控制的技术专利和知识产权，获得十年以上授权。
4. 按照GB/T 36637-2018要求开展供应链安全风险评估。
5. 建立并实施信息技术产品安全开发流程，明确开发管理要求、安全控制措施和人员行为准则等。
6. 制定所采购的信息技术产品及部件的可追溯性策略，记录并保留信息技术产品及部件的原产地、原供应方等相关信息。
7. 建立并实施规范的生产流程，采用访问控制、完整性和一致性校验等措施保障信息技术产品关键生产环节的安全，并对信息技术产品及部件进行唯一标识。
8. 制定物流服务供应方、物流路线的安全策略，记录和保留信息技术产品及部件的仓储、运输和交付等状态。
9. 在规定或者与需求方约定的期限内，不应终止提供安全维护；在需求方授权的范围内开展运行维护工作，保障信息技术产品运行维护过程中的数据安全，防止数据泄露、篡改、损毁，未经需求方同意不得向他人提供数据或将数据用于除运行维护以外的目的。
10. 提供中文版运行维护、二次开发等技术资料。

4.2 需求方安全要求

需求方应：

1. 通过采购文件、协议等要求供应方符合4.1的要求。
2. 建立和维护合格供应方目录，目录中的供应方应没有出现因政治、外交、贸易等因素中断信息技术产品、芯片等元器件、材料供应，停止软件授权、升级或技术支持服务的先例。
3. 从多个国家或地区获得信息技术产品及其部件，确保来源具有多样性。
4. 定期评估信息技术产品供应中断、停止授权、拒绝提供产品升级或技术支持服务的风险，确保供应链弹性；在约定的期限内，要求供应方提供信息技术产品供应链安全风险评估报告。

参 考 文 献

1. GB/T 22080－2008 信息技术 安全技术 信息安全管理体系要求
2. GB/T XXXXX-XXXX 信息安全技术 网络产品和服务安全通用要求（报批稿）
3. ISO/IEC 20243:2015 Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating Maliciously Tainted and Counterfeit Products
4. ISO/IEC 27036-3 Information technology — Security techniques—Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security
5. NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_