ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—Security criterion on supplier conduct of information technology products

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

本标准按照 GB/T 1.1—2009 的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、曙光信息产业股份有限公司、新浪网技术(中国)有限公司、北京奇虎科技有限公司、百度在线网络技术(北京)有限公司、北京瑞星科技股份有限公司、华为技术有限公司、中兴通讯技术有限公司、北京工业大学、中国信息安全研究院有限公司。

本标准主要起草人:高林、许东阳、姚相振、范科峰、王惠莅、蔡磊、罗锋盈、杨震、左晓栋、杨晨、石晓虹、王利俊、徐克超、叶润国、刘硕。

引　言

为贯彻落实《全国人民代表大会常务委员会关于加强网络信息保护的决定》的精神，加强信息技术产品用户相关信息保护，维护用户信息安全，本标准规定了信息技术产品供应方在相关业务活动中应遵循的基本安全准则。

信息安全技术　信息技术产品供应方行为安全准则

1　范围

本标准规定了信息技术产品供应方在提供信息技术产品过程中，为保护用户相关信息、维护用户信息安全应遵守的基本准则。

本标准适用于信息技术产品供应、运行或维护过程中的供应方行为管理，也可为信息技术产品的研发、运维及测评等提供依据。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

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：信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

3.2

信息技术产品供应方　information technology product supplier

提供信息技术产品的组织。

注：信息技术产品供应方包括生产商、销售商、代理商、集成商、服务商等。

3.3

用户相关信息　user related information

与自然人或法人有关的信息以及定义和描述这些信息的数据。

注：用户相关信息包括用户身份信息，以及用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据，系统运行过程产生日志等。

3.4

明示同意　expressed consent

用户信息主体明确授权同意，并保留证据。

3.5

远程控制　remote control

通过远程连接方式对用户产品实施的控制活动。

注：远程控制活动包括实现产品的启停、变更产品配置、改变产品运行状态、弹出对话框、自动远程升级、推送业务

数据等。

3.6

关键信息基础设施　national critical information infrastructure

关系国计民生的基础信息网络和重要信息系统，当这些网络或系统遭到攻击破坏时，会损害国家网络安全、经济安全、公众利益、公共安全等。

4　供应方行为安全准则

4.1　总则

信息技术产品供应方原则上不应收集、存储、处理用户相关信息，以及远程控制已提供给用户的产品和产品所在的信息系统，确有必要时，应遵循明示授权、最少够用、最小权限、安全可信的原则。

4.2　用户相关信息收集和处理的安全准则

供应方在收集和处理用户相关信息时：

a）　应在用户购买产品时明确告知用户收集用户相关信息的目的、用途和保护用户相关信息的策略，以及收集信息的类型、数量，存放地点、保存方式、保存期限、信息是否共享或转移等；

b）　应在用户购买使用产品时，提供禁止收集用户相关信息的方法，并告知禁止收集用户相关信息后产品缺失的功能；

c）　应在用户明示同意后，方可收集用户相关信息，并在收集用户相关信息时显示提示信息；

d）　应将收集的用户相关信息仅用于用户同意的目的和用途。未经用户同意，不得出售用户相关信息；

e）　应为用户提供查阅和修改其信息的方法、包括查阅修改流程、供应方相关联系人等信息；

f）　应采取必要技术和管理措施在收集、存储、处理时保护用户相关信息，防止其被泄露或滥用等；

g）　应在保存期限截至时或收到用户请求时，除非基于法律或监管原因，否则须彻底删除所有存储的用户相关信息；

h）　应制定用户相关信息泄露等事件时的应急预案，以便将影响和损失减到最低；

i）　应在我国境内存储、传输和处理在我国市场经营活动中收集的政府部门、关键信息基础设施相关信息；

j）　应为收集用户相关信息以及产品与供应方之间数据交互的行为提供检测、验证方法，包括所使用的端口和协议等信息，使用加密技术的，应在第三方机构检测验证时提供加密算法等；

k）　不应根据国外法律向境外机构提供中国用户信息或为获取相关信息提供便利条件。

4.3　远程控制用户产品的安全准则

供应方在远程控制用户产品时：

a）　应在用户购买使用产品前，明确告知用户远程控制行为的目的、用途等；

b）　应在用户购买使用产品前，提供禁止远程控制的方法，并告知用户禁止远程控制后产品缺失的功能；

c）　应经用户明示同意后，方可远程控制用户产品，并在远程控制用户产品时显示提示信息；

d）　应将远程控制活动仅用于用户同意的目的和用途，严格限制远程控制活动的频次和涉及产品系统范围；

e）　不应在产品中设置隐蔽接口，不应加载能够禁用或绕过安全机制的组件；

f）　不应在产品中存在未明示功能模块；

g）　应告知用户测试或维护接口，并给用户提供关闭测试或维护接口的方法；

h) 应采取必要技术和管理措施确保远程控制过程的安全性，并提供只能在限定的时间窗口使用特定账户进行访问的安全功能；

i) 应对远程控制所有输入输出的数据进行记录，并将所实施的远程控制活动载入日志以备日后审计；

j) 应为远程控制用户产品以及产品与供应方之间数据交互的行为提供检测、验证方法，使用加密技术的，应在第三方机构检测验证时提供加密算法等信息，并应告知第三方机构所使用的端口、协议等。

4.4 其他行为安全准则

供应方：

a) 不应通过技术手段限制用户选择其他供应方的产品、组件或技术；

b) 应为用户数据和业务在不同产品或信息系统间的迁移，提供必要的技术支持；

c) 应重视保护用户相关信息的工作，并为接触用户相关信息的人员提供培训；

d) 应在发生组织结构调整或服务外包时，及时告知用户并采取措施保证用户相关信息的安全。

参 考 文 献

[1] GB/T 27050.1—2006 合格评定供方的符合性声明 第1部分:通用要求
[2] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[3] GB/T 29244—2012 信息安全技术 办公设备基本安全要求
[4] ISO/IEC 15408—2009 信息技术 安全技术 信息技术安全性评估准则
[5] ISO/IEC 29100 信息技术 安全技术 隐私框架
[6] 欧盟关于在个人数据处理过程中保护当事人及此类数据自由流通的指令 1995/46/EC,1995
[7] NIST SP800—53 联邦信息系统安全与隐私控制措施
[8] NIST SP800—122 个人可识别信息(PII)机密性保护指南
[9] NIST Framework for Improving Critical Infrastructure Cybersecurity,2014.2