

ICS 35.080
L 77



中华人民共和国国家标准

GB/T 39770—2021

信息技术服务 服务安全要求

Information technology service—Service security requirements

2021-03-09 发布

2021-10-01 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	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 服务安全模型	2
5 服务安全总则	2
5.1 服务安全目标	2
5.2 服务安全原则	3
5.3 安全风险评估	3
5.4 服务需求方	3
5.5 服务提供方	3
6 服务生存周期安全要求	4
6.1 需求	4
6.2 设计	4
6.3 实现	4
6.4 运营	4
6.5 退出	4
7 服务能力要素安全要求	5
7.1 人员	5
7.2 过程	5
7.3 技术	6
7.4 资源	7
附录 A (资料性附录) 信息技术服务安全风险评估	8
附录 B (资料性附录) 服务安全角色和职责示例	9
参考文献	10

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:上海二零卫士信息安全有限公司、中国电子技术标准化研究院、北京护航科技股份有限公司、北京德信永道信息技术服务有限公司、中国电子科技网络信息安全有限公司、中国电信集团有限公司、北京银信长远科技股份有限公司、成都市人力资源社会保障信息中心、四川久远银海软件股份有限公司、成都信息化技术应用发展中心、北京伟仕佳杰信息技术服务有限公司、上海北亩企业管理咨询有限公司、上海安言信息技术有限公司、金税信息技术服务股份有限公司、成都清华永新网络科技有限公司、兴业数字金融服务(上海)股份有限公司、石家庄学院、平安科技(深圳)有限公司、南方电网广东佛山供电局、浙江大华技术股份有限公司、湖北工业职业技术学院、吉林省电子信息产品检验研究院、首都信息发展股份有限公司、江苏思特瑞信息技术有限公司、国网信通亿力科技有限责任公司。

本标准主要起草人:干露、查海平、张毅、张树玲、于浩、杨泉、董贵山、蒋涛、陈剑锋、张静、何昆、黄玉雯、陈杨、岳彩云、孙佩、付华茂、杨海涛、白璐、尹正茹、刘颀、钱伟峰、熊健淞、李霞、许志恒、李俊玲、李洋、沈勇、王晶、王晓清、干国胜、王丽明、吴芸、孙宇明、陈武。

信息技术服务 服务安全要求

1 范围

本标准提出了信息技术服务安全模型,规定了安全总则、生存周期和能力要素的安全要求。
本标准适用于信息技术服务提供方、服务需求方和第三方。

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 信息安全技术 术语

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

信息技术服务 information technology service

服务提供方为服务需求方开发、应用信息技术的服务,以及服务提供方以信息技术为手段提供支持服务需求方业务活动的服务。

注 1: 常见服务内容包括软件服务、硬件服务以及其他相关的服务。

注 2: 常见服务形态有信息技术咨询服务、设计与开发服务、信息系统集成实施服务、运行维护服务、数据处理和存储服务、运营服务、数字内容服务、呼叫中心服务及其他信息技术服务。

[GB/T 29264—2012,定义 2.1]

3.2

服务需求方 service acquirer

需要信息技术服务的组织机构或个人。

3.3

服务提供方 service provider

提供信息技术服务的组织机构或个人。

3.4

服务安全 service security

不因服务提供方相关服务要素的介入,以及供需双方的交互,导致对服务需求方的业务、资产、系统等造成损害的特性。

3.5

服务人员 service people

提供信息技术服务所需的人员。

3.6

服务过程 service process

提供信息技术服务时,合理利用必要的资源,将输入转化为输出的一组相互关联和结构化的活动。