ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 42447—2023

信息安全技术　电信领域数据安全指南

Information security technology—Data security guidelines for telecom field

2023-03-17 发布　　2023-10-01 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

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：中国移动通信集团有限公司、中国电子技术标准化研究院、中国信息通信研究院、中国联合网络通信集团有限公司、中国电信集团有限公司、中国人民银行数字货币研究所、成都思维世纪科技有限责任公司、中国科学院信息工程研究所、北京优炫软件股份有限公司、国家工业信息安全发展研究中心、北京东方通网信科技有限公司、北京亚鸿世纪科技发展有限公司、山谷网安科技股份有限公司、重庆邮电大学、北京明朝万达科技股份有限公司、闪捷信息科技有限公司、上海观安信息技术股份有限公司、北京邮电大学、慧盾信息安全科技(苏州)股份有限公司。

本文件主要起草人：张滨、张峰、杨亭亭、江为强、邱勤、张鑫月、魏薇、王光涛、温暖、于乐、上官晓丽、任兰芳、张媛媛、陈湉、胡影、粟栗、庞妹、何申、李文琦、刘明辉、静静、赵一宁、徐羽佳、孙艺、耿冠和、钟志成、黄志军、钟立、林飞、易永波、蔺思涛、宋玲娓、刘玉岭、柳彩云、崔婷婷、王世彪、瞿宏锋、赵蓓、金科、韩言妮、耿慧拯、顾慧琼、陈广辉、李春梅、左洪强、徐雨晴、谢江、赵帅、程渤、王晓波。

信息安全技术　电信领域数据安全指南

1　范围

本文件给出了开展电信领域数据处理活动的安全原则、通用安全措施，及在实施数据收集、存储、使用加工、传输、提供、公开、销毁等过程中宜采取的相应安全措施。

本文件适用于指导电信数据处理者开展数据安全保护工作，也适用于指导第三方机构开展电信数据安全评估工作。

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 41479—2022　信息安全技术　网络数据处理安全要求

3　术语和定义

GB/T 41479—2022 界定的以及下列术语和定义适用于本文件。

3.1

电信领域数据　telecom data

在电信领域业务经营活动中产生和收集的数据。

注 1：如用户身份信息、通话数据、位置数据、信令数据、基站建设及运维数据和网络优化数据等。

注 2：在不引起混淆的情况下，本文件中的“电信领域数据”简称“电信数据”。

3.2

电信数据处理者　telecom data processor

取得电信业务经营许可证，且在电信数据处理活动中自主决定处理目的、处理方式的电信业务经营者。

注：电信数据处理者包括基础电信业务经营者和互联网数据中心、互联网接入服务、在线数据处理与交易处理、互联网信息服务等增值电信业务经营者。

3.3

数据接收方　data receiver

数据处理中接收数据的组织或个人。

[来源：GB/T 41479—2022，定义 3.11]

4　缩略语

下列缩略语适用于本文件。

IP：互联网协议(internet protocol)

MAC：媒体访问控制(media access control)

SSL：安全套接层协议(secure socket layer)

VPN：虚拟专用网络(virtual private nsetwork)

4A：账号管理、授权管理、认证管理、审计管理(account、authentication、authorization、audit)

5 概述

电信数据处理者在开展数据处理活动过程中，提供适当的安全措施，以降低电信数据处理风险。

电信数据处理者按照有关要求和标准进行数据分类分级保护，在识别电信领域核心数据、重要数据、一般数据的基础上，采取数据安全措施，开展数据处理活动。第7章及第8章给出的安全措施分为一般措施和增强措施；处理一般数据时，电信数据处理者宜采取一般措施保护数据安全；处理重要数据和核心数据时，电信数据处理者宜在采取一般措施的基础上同时采取增强措施保护数据安全。

注1：重要数据和核心数据识别规则参考国家、行业相关规范，其他均属于一般数据。由于一般数据涵盖数据范围较广，电信数据处理者可根据生产经营需求对一般数据进行细化分级。

注2：对于未区分一般措施和增强措施的环节，一般数据、重要数据和核心数据参考同等措施进行保护。

6 安全原则

电信数据处理者遵循如下原则：

a) 安全三同步原则：在承载数据的相关平台设计、建设和运行过程中，做到数据安全保护措施的同步规划、同步建设、同步运行；

b) 分类分级保护原则：对数据进行分类分级，并根据类别属性、重要及敏感程度等差异性特征，采取适当的、与数据安全风险相适应的安全措施，保障数据安全；

c) 最小必要原则：在数据的收集、存储、使用、加工、传输、提供、公开、销毁等各处理活动开展过程中，所使用的数据类型及数据规模仅限定为业务开展所必需，且具有合法、正当、必要的目的；

d) 全生命周期管控原则：数据安全保护措施涵盖数据从产生到销毁的生命周期全过程；

e) 持续评估优化原则：对安全措施进行常态化、全面化安全评估，并根据评估结果持续动态优化数据安全保护措施。

7 电信数据通用安全措施

7.1 组织保障

电信数据处理者在组织保障方面宜采取以下安全措施。

a) 一般措施：

1) 明确数据安全管理职责部门，配备数据安全管理人员，制定数据安全制度规范和操作规程，配备数据安全技术能力；

2) 建立数据安全保护情况监督检查和考核管理制度，开展数据安全监督检查和考核管理。

b) 增强措施：

1) 建立数据安全工作体系，明确数据安全管理机构，设置数据安全管理专职岗位，建立数据安全管理机构与相关部门的协作机制；

2) 明确组织内数据安全管理第一责任人员等关键角色；

3） 梳理涉及重要数据和核心数据处理的工作岗位，明确岗位职责，签署数据安全责任书或保密协议。

7.2 数据分类分级

电信数据处理者在数据分类分级方面宜采取以下安全措施。

a） 一般措施：

1） 定期梳理数据资产，形成并及时更新数据资产清单，按照有关规定开展数据分类分级工作；

2） 根据业务需求、数据来源和用途等因素，划分组织机构数据类别，并根据数据资产变动和分类分级要求变动情况，及时更新数据资产清单。

b） 增强措施：形成更新重要数据和核心数据目录，按照有关规定开展目录备案工作。

7.3 权限管理

电信数据处理者在权限管理方面宜采取以下安全措施。

a） 一般措施：

1） 对开展数据处理活动的平台系统账号，明确审批流程和操作要求；

2） 遵循安全策略和最小授权原则，合理界定数据处理权限，设置相关岗位角色并确保职责分离，形成并定期更新数据处理权限记录表；

3） 对开展数据处理活动的平台系统，使用技术手段进行权限管理和账号管理（如 4A），同时控制超级管理员权限账户数量；

4） 涉及数据重大操作的，采取多人审批授权或操作监督方式。

b） 增强措施：

1） 明确重要数据和核心数据处理权限审批、登记方式和流程，控制权限范围，留存登记、审批记录；

2） 对开展重要数据和核心数据处理活动的平台系统，具备基于 IP 地址、账号与口令等的用户身份认证和多因子认证的能力，并配备权限管理保障功能。

7.4 日志留存

电信数据处理者在日志留存方面宜采取以下安全措施。

a） 对数据全生命周期处理过程进行日志记录，日志记录内容完整准确，内容包括操作时间、操作账号、处理方式、授权情况、操作对象和数据量级等。

b） 日志留存时间不少于 6 个月，定期对日志进行备份，日志记录可被查询检索。

7.5 安全审计

电信数据处理者在安全审计方面宜采取以下安全措施。

a） 一般措施：

1） 明确数据安全审计统筹部门，配备安全审计员，对权限分配审批、数据处理日志等开展安全审计工作；

2） 确定必要的数据安全审计策略，明确审计对象、审计内容和实施周期，开展数据重大操作、越权访问数据和远程访问数据等重点场景安全审计和数据分析；

3） 针对审计发现的问题及时处置、整改、跟踪复核，按照有关规定定期形成数据安全审计情

况总结。

b) 增强措施：

1) 开展数据安全审计技术能力建设(如4A)，细化常见风险和易发事件安全审计策略；

2) 按照有关规定定期形成重要数据、核心数据安全审计情况总结。

7.6 风险监测预警

电信数据处理者在风险监测预警方面宜采取以下安全措施：开展数据安全风险监测，对数据资产、数据处理环境、网络与系统设备、数据处理账号和内外部数据流动等实施监测巡查，对异常流动等行为进行排查和预警，及时采取补救措施。对可能造成较大及以上安全事件的风险，按照有关规定进行上报。

7.7 应急响应

电信数据处理者在应急响应方面宜采取以下安全措施。

a) 一般措施：

1) 制定数据安全事件应急预案，根据事件等级明确应急响应责任分工、工作流程和处置措施等；

2) 制定数据安全事件应急演练计划，针对数据泄露、丢失、窃取、损坏、滥用、篡改、非法访问和违规传输等典型数据安全事件定期开展演练，形成演练总结报告；

3) 发生数据安全事件后，按照应急预案及时开展应急处置，事件处置完成后，按照有关规定进行整改，形成总结报告并及时上报。

b) 增强措施：涉及重要数据和核心数据的安全事件，按照有关规定进行上报，同时开展事态跟踪分析，并及时采取相关措施降低事件影响。

7.8 安全评估

电信数据处理者在安全评估方面宜采取以下安全措施。

a) 一般措施：

1) 定期对本单位整体数据安全保护水平、重点业务与平台系统数据安全保障情况进行梳理和自查；

2) 对自查总结过程进行记录，形成总结报告，对发现的问题进行原因分析、明确改进措施和计划。

b) 增强措施：

1) 开展重要数据和核心数据风险评估，对于评估中发现的安全风险隐患，结合重要数据处理场景，及时采取有效应对措施消除风险隐患；

2) 按照有关规定向相关部门报送风险评估报告。

7.9 教育培训

电信数据处理者在教育培训方面宜采取以下安全措施。

a) 一般措施：

1) 制定数据安全岗位人员教育和培训计划，对数据安全相关岗位人员定期开展教育培训；

2) 明确数据安全岗位年度培训时长，并对参加培训的人员进行考核评定。

b) 增强措施：重要数据和核心数据处理岗位定期开展教育和培训，明确培训内容、培训时长、考核

评定等相关要求。

8 电信数据处理安全措施

8.1 数据收集

电信数据处理者开展数据收集活动，宜采取以下安全措施：

a) 一般措施：遵循合法、正当原则开展数据收集活动，规范数据收集渠道、流程和方式；

b) 增强措施：

1) 通过间接途径获取重要数据和核心数据的，与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任；

2) 开展重要数据和核心数据收集人员设备安全管理，采取安全防护手段防止针对数据收集设备的网络攻击。

8.2 数据存储

电信数据处理者开展数据存储活动，宜采取以下安全措施。

a) 一般措施：

1) 按照有关规定和用户约定进行数据存储，规范数据存储方式、流程，针对数据存储环境、存储平台系统实施安全管理；

2) 建立数据备份和恢复验证机制，保障存储数据的可用性和完整性。

b) 增强措施：

1) 采用校验技术、密码技术等措施保障数据安全存储；

2) 实施容灾备份和存储介质安全管理，定期开展数据恢复测试和灾难恢复演练，对备份数据的有效性和可用性进行检查和恢复验证。

8.3 数据使用加工

电信数据处理者开展数据使用加工活动，宜采取以下安全措施。

a) 一般措施：

1) 明确数据使用加工的审批流程及处理规则；

2) 利用数据进行自动化决策的，开展数据处理算法管理，保证自动化决策的透明度和结果的公平合理性。

b) 增强措施：使用访问控制、数据脱敏等技术措施保障重要数据使用加工过程的安全性。

8.4 数据传输

电信数据处理者开展数据传输活动，宜采取以下安全措施。

a) 一般措施：

1) 根据业务流程、网络部署和安全风险等情况，划分网络系统安全域。根据传输的数据类型、级别和应用场景等，明确数据安全策略并采取保护措施；

2) 制定数据传输接口安全管理工作规范，明确接口安全管理与保护措施。梳理接口情况，形成接口清单并定期更新，对监控发现存在安全问题或已下线的接口采取相应处理措施。

b) 增强措施：

1) 对跨网、跨安全域传输重要数据的活动，提前进行安全审批，并采取校验技术、密码技术、

安全传输通道(如 VPN)或者安全传输协议(如 SSL)等措施,保障重要数据传输的安全性;

2) 配备接口认证鉴权能力,支持通过 MAC 地址、IP 地址或端口号绑定等方式限制非授权或违规设备接入,具备接口安全监测能力,支持发现非授权或违规设备的接入,并进行告警和处置;

3) 具备接口流量限速、阻断等能力,支持对接口异常调用行为、重要数据异常传输事件等采取处置措施。

8.5 数据提供

电信数据处理者开展数据提供活动,宜采取以下安全措施。

a) 一般措施:

1) 明确数据提供的范围、类别、条件、程序等,定期梳理形成数据提供清单,确保清单内容完整准确;

2) 在服务合同或协议中明确数据安全保护条款,明确数据接收方可接触的数据范围、使用权限、目的及安全保护责任;

3) 数据提供涉及数据出境时,按照国家相关规定和相关标准的要求执行。

b) 增强措施:核验数据接收方数据安全保护能力,评估安全风险,并采取数据脱敏、数据加密等安全保障措施。

8.6 数据公开

电信数据处理者开展数据公开活动,宜采取以下安全措施:

a) 一般措施:明确数据公开的范围、类别、条件、程序等,在数据公开前分析研判可能对国家安全、公共利益产生的影响程度,存在重大影响的不得公开;

b) 增强措施:建立重要数据公开审批机制,对于法律法规要求公开的数据,使用数据脱敏技术实施保护。

8.7 数据销毁

电信数据处理者开展数据销毁活动,宜采取以下安全措施。

a) 一般措施:

1) 建立数据销毁制度,明确销毁场景、规则、流程和技术等要求,制定存储介质销毁处理规范,配备必要的数据销毁工具;

2) 数据批量销毁采用多人操作模式,单人不得拥有完整操作权限。

b) 增强措施:

1) 建立重要数据和核心数据销毁活动审批机制,设置销毁监督角色;

2) 销毁重要数据和核心数据后,不以任何理由、任何方式进行恢复,并按照有关规定更新备案。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[2] GB/T 35295—2017 信息技术 大数据 术语

[3] GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制

[4] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[6] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

[7] YD/T 3801—2020 电信网和互联网数据安全风险评估实施方法

[8] YD/T 3813—2020 基础电信企业数据分类分级方法

[9] 国家互联网信息办公室,数据出境安全评估办法,2022 年 7 月 7 日

[10] 中华人民共和国国务院令第 745 号,关键信息基础设施安全保护条例,2021 年 7 月 30 日

[11] 国务院关于印发促进大数据发展行动纲要的通知,国发〔2015〕50 号,2015 年 9 月 5 日

[12] NIST Special Publication 1500-2, NIST Big Data Interoperability Framework: Volume 2, Big Data Taxonomies, September 16, 2015

[13] NIST Special Publication 1500-4, NIST Big Data Interoperability Framework: Volume 4, Security and Privacy, September 16, 2015

[14] NIST Special Publication 1500-6, NIST Big Data Interoperability Framework: Volume 6, Reference Architecture, September 16, 2015