ICS 33.040
M10

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T ××××—××××

基础电信企业重要数据识别指南

Identification guide of key data for telecom operators

（报批稿）

××××-××-××发布　　××××-××-××实施

中华人民共和国工业和信息化部 发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 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这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准主要起草单位：中国信息通信研究院、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司。

本标准主要起草人：刘明辉、江为强、狄秋燕、国强、王渭清、朴鸿国、曹京、孙艺、曹咪、董胜亚、武姗姗、王雪琼、戚琳、秦博阳、陈淞、覃庆玲、魏亮、张峰、施阳、黄东豫、袁捷、李祥军、张滨、杨永平。

基础电信企业重要数据识别指南

1 范围

本标准给出了基础电信企业重要数据的定义、识别规则、识别方法和重要数据安全保护实施指导，并给出了基础电信企业重要数据示例。

本标准适用于持有基础电信业务经营许可证的企业在生产经营和管理活动中产生、采集、加工、使用或管理的数据，为基础电信企业重要数据安全管理工作提供指导。

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

YD/T 3802-2020 电信网和互联网数据安全通用要求

YD/T 3813-2020 基础电信企业数据分类分级方法

3 术语和定义

GB/T 25069 中界定的以及下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者非电子形式对信息的记录。

3.2

收集 collect

获得数据控制权的行为。

3.3

控制 control

有能力决定数据处理目的、方式等。

3.4

公开披露 public disclosure

向社会或不特定人群发布数据的行为。

4 缩略语

下列缩略语适用于本文件。

IP：网际协议（Internet Protocol）

IDC：互联网数据中心 （Internet Data Center）

ISP：互联网服务提供商 （Internet Service Provider）

VLAN：虚拟局域网 （Virtual Local Area Network）

WLAN：无线局域网 （Wireless Local Area Network）

IMS：IP 多媒体子系统 （IP Multimedia Subsystem）

5 基础电信企业重要数据的定义

基础电信企业的重要数据是指企业在运营中收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及公共利益密切相关的数据，特别是与国家基础通信网络安全密切相关的数据。

一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：

a） 危害国家安全、国防利益，破坏国际关系；

b） 损害国家财产、社会公共利益；

c） 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d） 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；

e） 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f） 危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；

g） 影响或危害国家经济秩序和金融安全；

h） 可分析出国家秘密或国家敏感信息；

i） 影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

6 基础电信企业重要数据的识别规则

基础电信企业应依据如下规则识别企业掌握的重要数据：

a） 基础电信企业掌握的能够反映通信行业整体情况的数据，如网络规划、建设、关键技术信息；

b） 基础电信企业掌握的通信网络基础资源信息，一旦被恶意利用，可能会导致国家基础通信网络中断，进而对国家安全和社会稳定造成重大影响；

c） 基础电信企业掌握的能够导致通信行业发生系统性风险的能够反映通信网络总体运行状况的数据，一旦完整性、保密性、可用性遭破坏可能对国家或社会带来负面影响的数据，如网络运行监控数据；

d） 基础电信企业掌握的通信网络与系统的设计、安全防护计划和策略方案，及其单元或设备选型、配置、软件等属性信息和脆弱性信息等；以及包括密码技术在内的其它与国家安全相关的单元、装置、设备、系统或计划、设计能力和缺陷信息；

e） 基础电信企业掌握的与意识形态、舆情等有关的文化安全相关信息；

f） YD/T 3813-2020 中四级数据中的用户相关数据比照重要数据管理；

g） 基础电信企业掌握的其他与国家公共安全、经济发展、社会稳定，以及公共利益密切相关的数据。

7 重要数据识别工作流程

7.1 数据分类分级

基础电信企业依据YD/T 3813-2020，全面梳理企业数据资源，完成数据分类分级识别与标识工作，然后实施重要数据判定工作。

7.2 重要数据判定

根据数据分类分级识别与标识的结果，重点针对安全级别较高（如四级和三级）的数据对象，依据重要数据识别规则，逐条对数据对象进行重要数据判定工作，判定流程见图1。

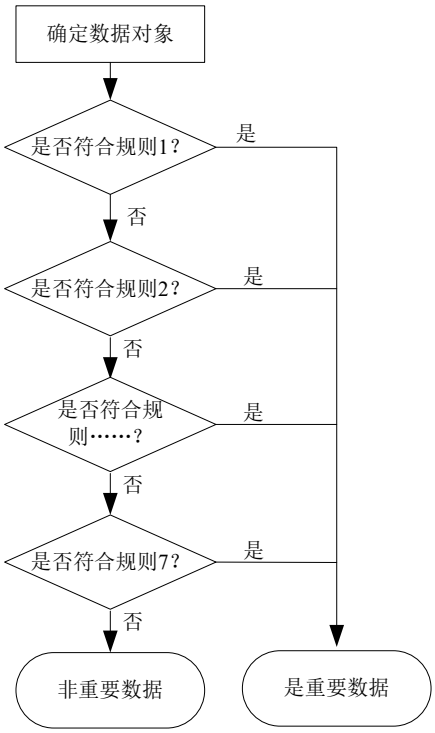

图1.重要数据判定流程

以规划建设类数据为例，基础电信企业的网络规划、建设信息能够反映通信行业整体情况，因此将规划建设类数据判定为重要数据。

按照以上判定流程，对YD/T 3813-2020附录A、附录B中所列三、四级数据逐一进行判定，形成基础电信企业重要数据示例，详见本标准附录A。其中，数据类别标号与YD/T 3813-2020附录A中一致。

7.3 重要数据标识

对判定为重要数据的数据对象，除分类分级标识外，增加重要数据标识。

7.4 重要数据清单

基础电信企业完成重要数据判定与标识后，输出企业重要数据清单，重要数据清单内容至少包括数据类型、内容描述、数据量、保存位置、保存期限、数据处理情况（数据处理目的、数据处理所涉及的信息系统）、数据对外提供情况（共享转让、公开披露、数据出境）、数据生命周期各环节安全措施配套情况。

8 基础电信企业重要数据安全保护指导

8.1 重要数据安全保护措施

除满足YD/T 3802-2020外，基础电信企业重要数据保护可以采取的安全措施如下：

a) 指定重要数据安全管理责任机构和负责人，落实重要数据安全保护责任。

b) 对重要数据进行标识，制定统一的重要数据安全策略，加强重要数据的安全管理。

c) 建立重要数据安全管理平台，采用自动化技术手段实现重要数据的统一登记、管理和使用监控等集中管理技术机制。

d) 对重要数据的采集/收集遵从合法、正当、必要、最小化原则；采集/收集过程中对数据源进行真实性校验，传输过程中采取加密、完整性保护等安全措施，防止重要数据被篡改、窃取、损毁。

e) 对重要数据的存储采用加密、备份、访问控制、安全审计等安全措施，保障重要数据存储安全。

f) 对重要数据的使用建立严格的审批流程，确保重要数据在国家法律法规要求允许范围内使用，不影响国家安全、社会公共利益，使用过程中应当采取访问控制、脱敏、异常行为监测、接口监控、安全审计等安全措施，防止重要数据被窃取、滥用。

g) 对重要数据的采集/收集、保存、使用、对外提供等全过程进行日志纪录，至少保存半年，对外提供环节日志记录保留两年，并采取防篡改、备份等措施保障日志数据的安全。

h) 对重要数据的采集/收集、保存、使用、对外提供等全过程进行实时安全审计。

i) 对重要数据的销毁设置安全策略和方法，严格按照策略执行审批、销毁、记录、检验等操作，并做好相关介质的管理和销毁。

8.2 重要数据评估

除满足YD/T 3802-2020外，基础电信企业重要数据安全评估机制包括：

a) 至少每半年进行一次针对重要数据收集使用情况的安全评估。

b) 对外提供、公开发布重要数据前，应开展安全评估；基础电信企业重要数据原则上应在境内存储，确需出境的，出境前应开展安全评估。

c) 安全评估报告应包括企业重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。

8.3 重要数据安全事件管理

基础电信企业应制定切实可行的数据安全应急预案，建立相应应急机制，定期开展应急演练，采取必要措施消除安全隐患。发生重要数据泄露、损毁、丢失等安全事件，或者发生数据安全事件风险明显加大时，基础电信企业应当立即采取补救措施，并及时按要求向电信管理机构上报。

附 录 A

（资料性附录）

基础电信企业重要数据示例

基础电信企业的重要数据示例如表 A.1 所示。

表 A.1 基础电信企业重要数据示例

2 企业自身相关数据		
2-1 网络与系统的建设与运行维护类数据		
子类	**范围**	**对应数据**
2-1-1 规划建设类数据	2-1-1-1 网络规划类	网络建设、网络规划研究、咨询等
	2-1-1-2 投资计划类	网络拓扑结构、新增设备信息、核心技术、设备采购、位置、性能、供应商等基础建设数据等
	2-1-1-3 项目管理类	项目建设方案、可研文件、设计文件等
2-1-2 网络与系统资源类数据	2-1-2-1 公共资源类数据	资源机架、DDM（数字诊断监视功能模块）、DDF（数字配线架）、ODM（光纤配线架连接模块）、ODF（光纤配线架）等基本信息
	2-1-2-2 传输资源类数据	2-1-2-2-1 传输外线基本信息：光交箱内的 ODF、跳线和光缆的数量、芯数、长度及分支接头盒等资源信息； 2-1-2-2-2 传输内线基本信息：传输专业涉及的机架、设备、ODF、DDF、光缆、跳线及标签等信息
	2-1-2-3 承载网资源	承载网设备及系统信息，如板卡、物理端口、逻辑端口、物理链路、逻辑链路、业务信息-IP 承载网、网段、IP 地址、VLAN 信息等
	2-1-2-4 核心网资源	分组域、电路域、IMS 系统等网元基本信息，包括 IP 地址、设备信息、信令链路等
	2-1-2-5 接入网资源	WLAN、无线网、有线网资源等基础信息，包括 AC（接入点）、AP（接入控制器）、热点、交换机、基站设备等

	2-1-2-6 IT 系统资源	业务支撑等平台相关的基本信息
	2-1-2-7 云资源	资源池、业务、服务器、虚拟机 VM、存储设备、负载均衡等基础信息，包括设备及软件信息、生命周期状态、所属机房等
2-1-3 网络与系统运维类	2-1-3-1 信令	信令数据
	2-1-3-2 路由	网络与系统的路由信息
	2-1-3-3 网段、网址、VLAN 划分	网段、网址、VLAN 分配与划分等信息
	2-1-3-4 设备监测、告警	设备监测、告警等信息
	2-1-3-5 信令监测	信令的监测信息
	2-1-3-6 流量监测	流量的监测信息
	2-1-3-7 运维日志	事件、地点、时间、操作、成功与否等信息
	2-1-3-8 运维系统账号密码等	运维系统的账号列表、密码等信息
	2-1-3-9 系统运行状况统计分析	网络及系统的运行统计分析数据等
2-1-4 网络安全管理类	2-1-4-1 安全审计记录	审计要求，审计决定、审计意见，审计结果通报，审计内参，审计报告及工作底稿等
	2-1-4-2 网络安全应急预案	应急预案、应急演练方案、应急物资管理等信息
	2-1-4-3	违法有害信息监测处置、舆情态势监测预警等数

	违法有害信息监测	据
	2-1-4-4 核心区域监控	核心区域视频监控记录数据等
	2-1-4-5 网络威胁数据	2-1-4-5-1 僵木蠕监控信息 2-1-4-5-2 移动恶意软件监控信息 2-1-4-5-3 IDC/ISP 告警信息 2-1-4-5-4 安全事件记录
2-3 企业管理数据		
2-3-1 发展战略与重大决策	2-3-1-1 发展战略	战略计划、战略风险评估等
	2-3-1-2 重大决策与重要会议	重大事项决策、重要干部任免、重大项目投资决策、大额资金使用相关的会议记录、纪要、材料、报告以及决策等
2-3-3 技术研发类（一旦泄露可能危害国家安全和社会稳定的核心技术、核心专利等）	2-3-3-1 技术管理	技术体制类规范、企业标准、技术成果、创新成果等
	2-3-3-2 技术研究报告	试验测试数据、试验分析报告等
	2-3-3-3 专利工作	专利申请技术交底书、专利布局相关报告、专利风险分析报告、专利纠纷应对策略等
2-3-5 生产经营类	2-3-5-1 财务预算	预算大盘子、各部门年度预算、季度滚动预算的相关数据及材料，关联交易额度、金融投资计划等
	2-3-5-2 业绩披露（公开披露前）	信息披露相关材料、业绩披露信息等
	2-3-5-4 生产经营数据	统计快报、年报数据、财务报表、生产经营分析材料、市场经营数据及分析报告、IT 系统生产经营报告等