

**中国移动数据分类分级及重要数据管控**

**实施指导意见**

**版本号 V1.0.0**

**中国移动通信有限公司**

**2021年8月**

目 录

[一、 引言 3](#_Toc21145)

[二、 总则 4](#_Toc3004)

[(一) 定义 4](#_Toc3656)

[(二) 参考依据 4](#_Toc12984)

[(三) 适用范围 5](#_Toc24419)

[三、 数据分类 5](#_Toc28896)

[(一) 用户相关数据 5](#_Toc1432)

[1. 用户身份和鉴权信息（A类） 5](#_Toc31954)

[2. 用户数据及服务内容信息（B类） 6](#_Toc1072)

[3. 用户服务相关信息（C类） 7](#_Toc16227)

[4. 用户统计分析数据（D类） 8](#_Toc4240)

[(二) 企业自身数据 8](#_Toc28839)

[1. 网络与系统的建设与运行维护类数据（E类） 8](#_Toc443)

[2. 业务运营类数据（F类） 10](#_Toc30184)

[3. 企业管理数据（G类） 10](#_Toc12505)

[4. 其他数据（H类） 12](#_Toc20618)

[四、 数据分级 12](#_Toc31512)

[(一) 分级原则 12](#_Toc11515)

[(二) 分级方法 12](#_Toc22363)

[(三) 分级表 13](#_Toc23059)

[(四) 分级管控要求 14](#_Toc18064)

[五、 重要数据 16](#_Toc29849)

[(一) 重要数据识别方法 16](#_Toc23472)

[(二) 重要数据识别表 17](#_Toc12229)

[(三) 重要数据管控要求 19](#_Toc16556)

1. 引言

为保障中国移动各类数据资产安全，保障用户合法权益，特制订本指南。

本指南主要针对中国移动数据安全管控分类分级进行了规范。内容主要包括：对公司数据进行分类，并在此基础上根据数据重要性和敏感程度进行分级，制订了不同级别的数据应遵循的管控实施要求，并对重要数据识别提出了建议。

本指南的解释权属于集团信息安全管理与运行中心。

1. 总则
   1. 定义

本指南所规定的数据范围为公司运营过程中通过网络（包括但不仅限于通信网、互联网、物联网等）收集、存储、传输、处理和产生的各种以电子或者其他方式记录的数据（涉及国家秘密的数据除外），包括用户相关数据和企业自身数据，商业秘密数据在满足本指导意见的基础上，按照公司商业秘密相关管理办法进行管理。

本指南所指的重要数据为企业在运营中收集、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：

（一）危害国家安全、国防利益，破坏国际关系；

（二）损害国家财产、社会公共利益；

（三）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；

（四）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；

（五）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；

（六）危害国家关键基础设施、关键系统、政府系统信息系统安全；

（七）影响或危害国家经济秩序和金融安全；

（八）可分析出国家秘密或国家敏感信息；

（九）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。

* 1. 参考依据

本指南主要参照了以下国家规范制度及指南：

* + 《中华人民共和国民法典》
  + 《中华人民共和国网络安全法》
  + 《中华人民共和国数据安全法》
  + 《中国人民共和国个人信息保护法》
  + 《中华人民共和国电信条例》
  + 《电信和互联网用户个人信息保护规定》（工信部2013年第24号令）
  + 《信息安全技术 个人信息安全规范》，（GB/T 35273-2020）
  + 《基础电信企业数据分类分级方法》，（YD/T 3813-2020）；
  + 《基础电信企业重要数据识别指南》，(YD/T 3867-2021)；

同时，参照了以下公司内部规范制度：

* 《中国移动通信集团有限公司数据安全管理办法（试行）》
  1. 适用范围

本指南适用于集团公司各部门、省/自治区/直辖市公司、直属单位、分支机构、专业分公司、业务基地（以下简称各单位），是各单位开展数据分类分级安全管控工作的基本依据。

1. 数据分类

根据中国移动生产经营管理现状和企业自身管理特点，可将数据资源分为两大类以便于对数据进行统一管理及推广应用，具体包括：

（一）用户相关数据，主要涉及用户身份和鉴权信息、用户数据及服务内容信息、用户服务相关信息、用户统计分析数据。

（二）企业自身数据，包括网络与系统的建设与运行维护类数据、业务运营类数据、企业管理数据、其他数据。

各单位可在本分类方法的基础上，根据自身情况进一步补充细化。

* 1. 用户相关数据
     1. 用户身份和鉴权信息（A类）

用户身份和鉴权信息包括用户身份和标识信息、用户网络身份鉴权信息。

表一 A类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| A1.用户身份和标识信息 | A1-1：自然人身份标识 | 客户姓名、证件类型及号码、驾照编号、银行账户等 |
| A1-2：网络身份标识 | 联系电话、邮箱地址（如139邮箱地址）、网络客户编号、即时通信账号（如飞信号）、网络社交用户账号等可以精确标识网络用户或通信用户的信息 |
| A1-3：用户基本信息 | 客户职业、工作单位、年龄、性别、籍贯、兴趣爱好等 |
| A1-4：实体身份证明 | 身份证、护照、驾照、营业执照等证件影印件等；个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等个人生物识别信息 |
| A1-5：用户私密信息 | 揭示个人种族、家属信息、居住地址、宗教信仰、基因、个人健康、私人生活等有关的用户私密信息；《征信业管理条例》等法律、行政法规规定禁止公开的用户其他信息 |
| A1-6：集团客户信息 | 客户实体编号、集团客户编号、集团客户名称、集团客户负责人\联系人信息、IDC/ISP企业客户信息等可以精确标识定位具体实体客户的信息、集团客户所在省市、所在行业、集团签约时间及协议到期时间等 |
| A2：用户网络身份鉴权信息 | A2-1：用户密码及关联信息 | 用户网络身份密码及关联信息，如：手机客服密码、139邮箱密码、飞信密码、移动wlan密码、和包等交易密码，以及这些密码关联的密码保护答案等 |

* + 1. 用户数据及服务内容信息（B类）

用户数据及服务内容信息包括服务内容和资料数据、联系人信息。

表二 B类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| B1：服务内容和资料数据 | B1-1：服务内容数据 | **电信网服务内容数据**：短信、彩信、话音等通信内容；  **移动互联网服务内容信息**：包括：飞信、融合通信、139邮箱等移动互联网服务所涉及通话内容、即时通信内容、群内发布内容、数据文件、邮件内容、用户上网访问内容等；用户云存储、SDN、IDC等存储或缓存的非公开的私有文字、多媒体等资料数据信息 |
| B1-2：联系人信息 | 用户通讯录、好友列表、家庭网、V网列表、群组列表等用户资料数据 |

* + 1. 用户服务相关信息（C类）

用户服务相关信息主要包括用户服务使用数据、设备信息。

表三 C类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| C1：用户服务使用数据 | C1-1：业务订购关系 | **基本业务订购关系**：品牌、套餐定制等情况  **增值业务订购关系**：139邮箱、飞信、和通讯录、来显、彩铃、和包等增值业务的注册、修改、注销等 |
| C1-2：服务记录和日志 | **服务详单及信令**：包括语音、短信、彩信、宽带和上网日志详单、2G/3G/4G/5G用户面XDR及信令面XDR等，内含主叫号码、主叫归属地、被叫号码、开始通信时间、时长、流量等信息  **移动互联网服务记录**：包括Cookie内容、上网日志、连接APP等，内含主叫号码、网址、网购记录等 |
| C1-3：消费信息和账单 | **消费信息**：停开机、入网时间、在网时间、积分、预存款、信用等级、信用额度、缴费情况、付费方式、和包余额、交易历史记录等  **账单**：每月出账的固定费用、通信费用、欠费信息、数据费用、代收费用等 |
| C1-4：位置数据 | 精确位置信息(如小区代码、基站号、基站经纬度坐标等)  大致位置信息(如地区代码、城市代码等) |
| C1-5：违规记录数据 | 用户违规记录，包括垃圾短信、骚扰电话等记录、黑名单、灰名单等 |
| C2：设备信息 | C2-1：终端设备标识 | 唯一设备识别码IMEI、设备MAC地址、SIM卡IMSI信息等可以精确标识定位具体设备的信息 |
| C2-2：终端设备资料 | 终端型号、品牌、厂商、OS类型、预置\安装软件应用、使用时长等 |

* + 1. 用户统计分析数据（D类）

用户统计分析数据主要包括用户使用习惯和行为分析数据、用户上网行为相关统计分析数据。

表四 D类数据详细内容

|  |  |  |
| --- | --- | --- |
| D1：用户统计分析数据 | D1-1 用户使用习惯和行为分析数据 | 用户偏好、消费习惯，通话、短信频次、上网等数量与频次等。 |
| D1-2 用户上网行为相关统计分析数据 | 用户网络行为、用户画像等 |

* 1. 企业自身数据

1. 网络与系统的建设与运行维护类数据（E类）

网络与系统的建设与运行维护类数据分为规划建设类数据、网络与系统资源类数据、网络与系统运维类数据、网络安全管理类数据。

表五 E类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| E1 网络规划建设类数据 | E1-1 网络规划类数据 | 网络建设、网络规划研究、咨询等 |
| E1-2 投资计划类数据 | 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 |
| E1-3 项目管理类数据 | 项目建设方案、可研文件、设计文件等 |
| E2 网络与系统资源类数据 | E2-1 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（光配线架连接模块)、ODF（光纤配线架）等基本信息 |
| E2-2 传输资源类数据 | 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； 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 |
| E2-3 承载网资源类数据 | 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 |
| E2-4 核心网资源类数据 | 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 |
| E2-5 接入网资源类数据 | 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 |
| E2-6 IT系统资源类数据 | 业务支撑等平台相关的基本信息 |
| E2-7 云资源类数据 | 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 |
| E3 网络与系统运维类数据 | E3-1 信令 | 信令数据 |
| E3-2 路由 | 网络与系统的路由信息 |
| E3-3 网段、网址、VLAN 划分 | 网段、网址、 VLAN 分配与划分等信息 |
| E3-4 设备监测、告警 | 设备监测、告警等信息 |
| E3-5 信令监测 | 网络运维相关设备信令监测信息、原始XDR信息 |
| E3-6 流量监测 | 网络运维相关设备流量监测信息 |
| E3-7 运维日志 | 各类操作日志数据、工单处理记录等 |
| E3-8 运维系统账号密码等 | 运维系统的账号列表、密码等信息 |
| E3-9 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 |
| E4 网络安全管理类数据 | E4-1 安全审计记录 | 网络安全管理相关的安全核查报告、核查意见、核查决定、核查结果通报等 |
| E4-2 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 |
| E4-3 违法有害信息监测 | 违法有害信息监测处置、舆情态势监测预警等数据 |
| E4-4 核心区域监控 | 核心区域视频监控记录数据等 |
| E4-5 网络威胁数据 | 僵木蠕监控信息、移动恶意软件监控信息、IDC/ISP 告警信息、安全事件记录 |

1. 业务运营类数据（F类）

业务运营类数据包括业务运营服务数据和公开业务运营服务数据。

表六 F类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| F1 业务运营服 务数据 | F1-1 产品信息 | 产品 ID、套餐设置、销售品 ID 等 |
| F1-2 渠道信息 | 渠道（佣金、业务受理等）数据， CP/SP（结算、业务订购等）数据等 |
| F1-3 客户服务信息 | 满意度调研数据、分析报告，实体渠道第三方监测、营业厅服务质检等信息 |
| F1-4 营销信息 | 充值数据，精准营销和服务应用号码及标签，各类预缴、促销、捆绑和营销奖励用户号码，终端业务各类指标完成数据、终端经营日常生产数据等 |
| F2 公开业务运 营服务数据 |  | 产品数字内容业务运营数据：业务平台文本、视频、知识库等数字内容运营数据等； 资费信息、公开的业务运营数据等 |

1. 企业管理数据（G类）

企业管理数据包括发展战略与重大决策、业务发展类数据、技术研发类数据、运行管理类数据、生产经营类数据、综合管理类数据。

表七 G类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| G1 发展战略与重大决策 | G1-1 发展战略 | 战略计划、战略风险评估等 |
| G1-2 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 |
| G2 业务发展类数据 | G2-1 市场策略 | 市场发展策略、市场经营专项研究报告、市场发展指导意见等 |
| G2-2 营销管理 | 品牌及传播推广策略、业务发展策略、管理办法、高端客户名单、白名单等 |
| G2-3 资费管理 | 资费方案、资费管理等信息 |
| G2-4 产品发展策略 | 产品试点方案、试商用方案、业务融合方案等 |
| G3 技术研发类数据 | G3-1 技术管理 | 技术体制类规范、企业标准、技术成果、创新成果等 |
| G3-2 技术研究报告 | 试验测试数据、试验分析报告等 |
| G3-3 专利相关信息 | 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 |
| G4 运行管理类数据 |  | 运行管理相关的规程、操作指南、计划等 |
| G5 生产经营类数据 | G5-1 财务预算 | 公司年度预算、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 |
| G5-2 业绩披露 | 信息披露相关材料、业绩披露信息等 |
| G5-3 考核相关信息 | 经营业绩考核办法、考核结果等信息 |
| G5-4 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 |
| G6 综合管理类数据 | G6-1 人力资源 | 人员管理数据、机构管理数据、劳动用工管理数据、薪酬管理数据等 |
| G6-2 财务信息 | 收入、利润、预算、决算数据等（分公开前后） |
| G6-3 监督管理信息 | 审计、纪检、巡视等部门为履行监督管理职能，监督管理要求、决定、意见，过程底稿、结果报告、通报等 |
| G6-4 办公自动化 | 邮件、行政文件、签报等信息 |
| G6-5 采购 | G6-5-1 招投标数据（分公开前后）：采购招标的技术规范相关信息、招标及采购该过程信息、投标、订单等信息 G6-5-2 物资数据： 采购物资数量、类型等信息  G6-5-3 业务合作类数据：合作方信息、合同台账、各类采购合同（协议）、供应商考核等信息 |

1. 其他数据（H类）

其他数据主要为合作方提供数据。

表八 H类数据详细内容

|  |  |  |
| --- | --- | --- |
| **子类** | **范围** | **对应数据** |
| H1 合作方提供数据 |  | 音视频等互联网内容数据 |

1. 数据分级
   1. 分级原则

数据分级应按照数据重要程度和敏感程度，依据以下原则：

* 时效性原则：数据分级具有一定的有效期。数据的级别可能因时间变化按照一些预定的安全策略发生改变。
* 就高不就低原则：如果同一批数据中各属性或字段的分级不同，需要按照定级最高的属性或字段的级别一并实施安全管控，即“就高不就低”。
* 关联叠加效应原则：对于数据关联后可能产生更高级别数据的场景，关联后的数据级别应高于原始数据。

根据公司内部数据特点，建议按照数据重要程度和敏感程度由高到低划分为四级。各单位可在本分级方法的基础上，根据自身情况进一步补充细化。地方政府、行业监管部门有其他管控要求的，从其规定。

* 1. 分级方法

进行数据分级时，应考虑其安全属性（机密性、完整性、可用性）遭到破坏时造成的影响的客体，包括：国家安全和社会公共利益， 企业利益和用户利益。

1) 对国家安全和社会公共利益的影响应考虑数据一旦未经授权披露、丢失、滥用、篡改、破坏、泄露、销毁，可能造成的后果对国家安全和社会公共利益的影响程度。

2) 对企业利益的影响应考虑如下3个方面：

* 业务影响：应考虑数据安全事件发生后对生产业务造成的影响。
* 财务影响：应考虑数据安全事件发生后导致的财务损失。包括：直接损失（收入受损、缴纳罚款、赔偿金或其他资源损失等）和恢复成本（比如恢复数据、恢复业务、消除影响、安抚/挽回客户等涉及的资金或人工成本等）。
* 声誉影响：应考虑数据安全事件发生后被外界所知所造成的声誉受损，包括客户信任度、公司形象、行业声誉、社会认同感等。

3) 对用户利益的影响应考虑如下用户数据一旦发生安全事件后，对用户财产、声誉、生活状态以及生理和心理等方面产生的影响。

* 1. 分级表

表九 数据分级表

|  |  |
| --- | --- |
| 类别 | 子类及范围 |
| 第4级 | A1-4 实体身份证明、 A1-5 用户私密信息、A2-1 用户密码及关联信息、 B1-2 联系人信息、  E1 网络规划建设类数据（关键系统，发布前）、 E2 网络与系统资源类数据（关键系统）、 E3 网络与系统运维类数据（关键系统）、 E4 网络安全管理类数据（关键系统） |
| 第3级 | A1-1 自然人身份标识、B1-1 服务内容数据、C1-2 服务记录和日志、C1-4 位置数据、 D1-1 用户使用习惯和行为分析数据、 D1-2 用户上网行为相关统计分析数据、 E1 网络规划建设类数据（等保3级及以上系统，发布前）、E2 网络与系统资源类数据（等保3级及以上系统）、 E3 网络与系统运维类数据（等保3级及以上系统）、 E4 网络安全管理类数据（等保3级及以上系统）、G1 发展战略与重大决策、G2 业务发展类数据、 G3 技术研发类数据、 G5 生产经营类数据、G6-1 人力资源、G6-2 财务信息（公开前）、G6-3 监督管理信息、 G6-5-1 招投标数据（公开前） |
| 第2级 | A1-2 网络身份标识、 A1-3 用户基本信息、A1-6 集团客户信息、C1-1业务订购关系、C1-3 消费信息和账单、 C2-1 终端设备标识、C2-2 终端设备资料、 E1 网络规划建设类数据（关键、等保3级及以上系统发布后、其它系统发布前后）、E2 网络与系统资源类数据（等保3级以下系统）、 E3 网络与系统运维类数据（等保3级以下系统）、 E4 网络安全管理类数据（等保3级以下系统）、 F1-2 渠道信息、 F1-3 客户服务信息、 F1-4 营销信息、G4 运行管理类数据、G6-4 办公自动化、G6-5-1 招投标数据（公开后）、 G6-5-2 物资数据、G6-5-3 业务合作类数据、H1 合作方提供数据 |
| 第1级 | C1-5 违规记录数据 F1-1 产品信息、F2 公开业务运营服务数据、G6-2 财务信息（公开后） |

* 1. 分级管控要求

应对各级数据建立适当的管控措施，通过自动识别和人工识别相结合的方式对数据进行识别，实现数据的分类分级，并对数据进行分类分级标识。除满足《中国移动通信集团有限公司数据安全管理办法（试行）》的要求外，各级数据还应满足如下的管控要求。涉及公司商业秘密的数据还需同时满足其相关的管理要求。

表十 分类分级管控要求表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 管控要求 | 第1级 | 第2级 | 第3级 | 第4级 |
| 数据收集环节 | 应对接入的数据源收集设备或系统进行鉴别，采用数据源鉴别技术防止数据源伪冒。 | √ | √ | √ | √ |
| 对收集行为进行日志记录和安全审计，并对超规模、超范围收集等异常行为进行告警。 |  | √ | √ | √ |
| 限制收集过程中使用的临时存储文件，将缓存区域纳入统一安全管控范畴，不得任意修改存储区域地址，对存储区域的方案实施最小权限原则，只允许收集、上传应用程序使用临时存储区域。 |  |  | √ | √ |
| 数据传输环节 | 应建立机制对系统间数据传输进行管控，在传输前由数据发送方提出明确的管控要求、接收方需配备不低于发送方的管控手段，通过正式的文件明确双方的责任。 | √ | √ | √ | √ |
| 传输前应对接入的设备进行身份鉴别。 | √ | √ | √ | √ |
| 应对数据传输过程实施数据完整性校验。 | √ | √ | √ | √ |
| 对数据进行加密后传输或通过加密信道传输，保证数据传输的保密性。 |  | √ | √ | √ |
| 使用技术手段防止数据传输过程中发生篡改。 |  |  | √ | √ |
| 数据存储环节 | 应提供完整性保护，并提供完整性校验机制，以发现存储阶段的数据损坏和丢失。 | √ | √ | √ | √ |
| 针对分布式存储系统，应开启身份鉴别机制。 | √ | √ | √ | √ |
| 应对数据的存储、访问情况进行日志记录。 | √ | √ | √ | √ |
| 应对数据存储设备和系统进行必要的安全管控，包括设备操作终端的鉴权机制、系统的访问控制、系统配置的安全基线等。 |  | √ | √ | √ |
| 应完善存储系统日志内容，记录访问账号、访问IP、执行操作、涉及资源、权限鉴别等内容，日志存储半年以上。 |  | √ | √ | √ |
| 应对存储系统的维护终端实施权限管控，对运维人员实施细粒度权限管控，普通运维人员不能对存储系统上的业务数据进行读写操作。 |  | √ | √ | √ |
| 应对所有存储设备的外接存储介质进行严格管控，限制外插闪存盘、移动硬盘等移动存储介质。 |  |  | √ | √ |
| 对备份的数据执行和数据源采用同样的安全管控措施，包括访问控制、完整性校验等。 |  |  | √ | √ |
| 对数据进行加密存储。 |  |  |  | √ |
| 数据使用环节 | 依据权限最小化原则分配账号权限，通过技术手段（如4A管控等）统一实现账号认证和权限分配；应使用系统或应用权限分配功能对不同等级的数据设置不同的访问权限，不同用户只能访问与自己职责对应的数据。 | √ | √ | √ | √ |
| 应支持对于数据库、文件的细粒度授权方式，可针对不同用户仅授权业务所需的最少功能。 |  | √ | √ | √ |
| 提供基于用户名、IP地址等方式的认证及细粒度权限控制。 |  |  | √ | √ |
| 应对数据的访问、导入导出等使用行为进行日志记录，应针对数据访问、数据分析、系统运维等数据使用过程，保留应用程序登录、访问以及数据使用操作的日志记录。 | √ | √ | √ | √ |
| 应对数据的批量导出进行审批授权，并保留审批记录。 | √ | √ | √ | √ |
| 对数据的【高风险】操作实行严格管控，通过技术手段（如金库模式等）或者建立审批机制限制人员直接访问业务数据。 |  | √ | √ | √ |
| 应限制所有特权操作，查询用户数据时，确保所有查询操作经过用户授权，并留存授权记录，防止在未经用户授权的情况下进行查询操作。 |  | √ | √ | √ |
| 应对数据导入导出操作进行限定，保证仅在业务需要的合理必要范围内执行数据导入导出操作。 |  | √ | √ | √ |
| 应对API接口进行强制访问控制，所有授权调用的API，均需在后台可被查询管理，并对超频次调用、访问流量异常等行为进行监测及阻断。 |  | √ | √ | √ |
| 部署监控方案，提高对危险行为的处置能力和响应速度；基于机器学习算法对数据使用过程进行多维度分析，实现应用、用户行为的关联分析，预判危险行为，并及时处理。 |  |  | √ | √ |
| 数据共享环节 | 对数据中个人信息开放共享需经过用户授权，经匿名化后无法识别或关联个人信息主体的除外。 | √ | √ | √ | √ |
| 应做好授权与访问控制，对外部接口的访问进行统一认证，进行日志记录，定期对日志进行安全审计。 | √ | √ | √ | √ |
| 应采用多租户、消息订阅、数据共享API封装等安全的共享方式，避免上层应用对数据的越权访问。 |  | √ | √ | √ |
| 采取数字水印等技术手段，保证共享数据可以进行溯源。 |  | √ | √ | √ |
| 持续对共享中的数据进行安全态势监测，当发现违反用户行为规律的操作发生时，进行告警，对高危操作进行实时阻断。 |  | √ | √ | √ |
| 禁止第四级数据对外共享。 |  |  |  | √ |
| 数据销毁环节 | 建立数据销毁管理流程，由数据管理部门对数据销毁操作进行审批，并留存审批记录。 | √ | √ | √ | √ |
| 对数据销毁进行效果验证，提供节点失效监测等基础能力；采取下列两种以上的方式对数据进行销毁：删除文件、格式化硬盘、文件粉碎机、文件覆写、消磁等，确保彻底删除、不可恢复。 |  | √ | √ | √ |
| 存放3级及以上数据的存储服务器、磁盘阵列需要替换时，应对硬盘进行物理销毁，确保数据彻底删除、不可恢复。 |  |  | √ | √ |

1. 重要数据
   1. 重要数据识别方法

可依据如下规则识别企业掌握的重要数据：

* 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。
* 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。
* 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。
* 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。
* 企业掌握的与意识形态、舆情等有关的文化安全相关信息。
* 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。
  1. 重要数据识别表

基于重要数据的定义，依据识别方法，识别的重要数据主要集中为网络与系统的建设与运行维护类数据、企业管理类数据中的部分数据。

表十一 重要数据详细内容

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 子类 | 范围 | 对应数据 |
| E 网络与系统的建设与运行维护类数据（关键系统、等保3级及以上系统） | E1 网络规划建设类数据 | E1-1 网络规划类数据 | 网络建设、网络规划研究、咨询等 |
| E1-2 投资计划类数据 | 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 |
| E1-3 项目管理类数据 | 项目建设方案、可研文件、设计文件等 |
| E2 网络与系统资源类数据 | E2-1 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（光配线架连接模块)、ODF（光纤配线架） 等基本信息 |
| E2-2 传输资源类数据 | 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； 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 |
| E2-3 承载网资源类数据 | 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 |
| E2-4 核心网资源类数据 | 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 |
| E2-5 接入网资源类数据 | 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 |
| E2-6 IT系统资源类数据 | 业务支撑等平台相关的基本信息 |
| E2-7 云资源类数据 | 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 |
| E3 网络与系统运维类数据 | E3-1 信令 | 信令数据 |
| E3-2 路由 | 网络与系统的路由信息 |
| E3-3 网段、网址、VLAN 划分 | 网段、网址、 VLAN 分配与划分等信息 |
| E3-4 设备监测、告警 | 设备监测、告警等信息 |
| E3-5 信令监测 | 信令监测信息、原始XDR信息 |
| E3-6 流量监测 | 流量监测信息 |
| E3-7 运维日志 | 各类操作日志数据、工单处理记录等 |
| E3-8 运维系统账号密码等 | 运维系统的账号列表、密码等信息 |
| E3-9 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 |
| E4 网络安全管理类数据 | E4-1 安全审计记录 | 网络安全管理相关的安全检查通知、检查报告、检查意见、检查决定、检查结果通报 |
| E4-2 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 |
| E4-3 违法有害信息监测 | 违法有害信息监测处置、舆情态势监测预警等数据 |
| E4-4 核心区域监控 | 核心区域视频监控记录数据等 |
| E4-5 网络威胁数据 | 僵木蠕监控信息、移动恶意软件监控信息、IDC/ISP 告警信息、安全事件记录 |
| G 企业管理数据 | G1 发展战略与重大决策 | G1-1 发展战略 | 战略计划、战略风险评估等 |
| G1-2 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 |
| G3 技术研发类数据 | G3-1 技术管理 | 技术体制类规范、企业标准、技术成果、创新成果等 |
| G3-2 技术研究报告 | 试验测试数据、试验分析报告等 |
| G3-3 专利相关信息 | 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 |
| G5 生产经营类数据 | G5-1 财务预算 | 公司年度预算、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 |
| G5-2 业绩披露 | 信息披露相关材料、业绩披露信息等 |
| G5-4 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 |

* 1. 重要数据管控要求

重要数据在满足分级管控技术要求的同时，还应遵循如下要求实施保护：

(1) 应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。

(2) 应建立企业重要数据清单，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。

(3) 应对重要数据采取统一登记、管理和使用监控等集中管理技术机制。

(4)使用重要数据应当建立严格的内部审批流程，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。

(5) 应对重要数据的采集/收集、存储、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。

(6) 应对重要数据的采集/收集、存储、使用、对外提供等全过程进行定期安全审计。

(7) 应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）应当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。对外提供、公开发布重要数据前，应当开展安全评估；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。

（9）应当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，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。

用户相关数据中的第四级数据需比照重要数据管理。