ICS 33.040
M10

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T 3813—2020

基础电信企业数据分类分级方法

Data classification and grading method of basic telecommunication enterprises

2020-12-25 发布　　2020-12-25 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给出的规则起草。

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、上海观安信息技术股份有限公司、成都思维世纪科技有限责任公司、中国移动通信集团设计院有限公司、北京亚鸿世纪科技发展有限公司、北京微智信业科技有限公司、北京优炫软件股份有限公司。

本标准主要起草人：刘明辉、陈湉、朴鸿国、曹京、戚琳、秦博阳、覃庆玲、魏亮、江为强、狄秋燕、孙艺、曹咪、国强、董胜亚、武姗姗、王雪琼、于乐、邱勤、贾强、常玲、赵蓓、杜雪涛、张峰、李祥军、袁捷、施阳、张滨、杨永平、黄东豫、邹静洁、戴荣鑫、张超、刘晓光、钟立、钟志成、张晨、易永波、熊翱、李侠、崔婷婷、张春林、吴志辉、黄志军、周踊、芦京洪。

基础电信企业数据分类分级方法

1 范围

本标准规定了基础电信企业数据分类分级原则、数据分类工作流程和方法，数据分级方法，并给出基础电信企业数据分类分级示例。

本标准适用于基础电信企业的数据分类分级。本标准不适用于涉及国家秘密的数据。

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 信息安全技术 术语

GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 25069和GB/T 29246界定的以及下列术语和定义适用于本文件。

3.1

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

3.2

机密性 confidentiality

数据不能被未授权的个人、实体或者过程利用或知悉的特性。

3.3

可用性 availability

根据授权实体的要求可访问和使用的特性。

3.4

完整性 integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

3.5

网络 network

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.6

网络数据 network data

通过网络收集、存储、传输、处理和产生的各种电子数据。

3.7

非网络数据 non network data

非经网络收集、存储、传输、处理和产生的各种电子或非电子数据。

4 缩略语

下列缩略语适用于本文件。

IMEI：移动设备国际身份码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identification Number）

IP：网际协议（Internet Protocol）

MAC：介质访问控制（Media Access Control）

SIM：用户身份识别模块（Subscriber Identity Module）

5 适用范围

本标准所规定的数据范围包括基础电信企业生产经营和管理活动中产生、采集、加工、使用或管理的网络数据和非网络数据。

6 分类分级原则

基础电信企业数据分类分级应依据如下原则：

a） 安全性原则

从利于数据安全管控的角度对数据进行分类分级

b） 稳定性原则

分类分级设置在相当长一个时期内是稳定的，对各类数据的涵盖面广，包容性强。

c） 可执行性原则

宜避免对数据进行过于复杂的分类分级规划，保证数据分级使用和执行的可行性。后续相关的安全防护要求都在此分类分级的基础上开展。

d） 时效性原则

数据的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。

e） 自主性原则

基础电信企业可根据自身的数据管理需要，例如战略需要、业务需要、对风险的接受程度等，按照数据分类原则进行分类之后，按照数据分级方法自主确定更多的数据层级，但不宜将高敏感度数据定为低敏感度级别。

f） 合理性原则

数据级别宜具有合理性，不能将所有数据集中划分一两个级别中，而另外一些没有数据。级别划定过低可能导致数据不能得到有效保护；级别划定过高可能导致不必要的业务开支。

g） 客观性原则

数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其分级，已经分级的数据是可以复核和检查的。

h） 就高不就低原则

不同级别的数据被同时处理、应用时且无法精细化管控时，应按照其中级别最高的要求来实施保护。

i） 关联叠加效应原则

对于非敏感数据关联后可能产生敏感数据的场景，关联后的数据级别应高于原始数据。

7 数据分类分级工作流程

7.1 建立数据分类分级组织保障

数据分类分级工作的开展需要有组织保障，企业应明确：

a） 数据分类分级的决策机构和最高责任人。决策机构负统筹和决策职责，决策数据分类分级工作的目标、内容、标准规范等。决策机构的最高责任人对数据分类分级工作负全面领导责任。

b） 数据分类分级的牵头部门。牵头部门负责牵头推动数据分类分级工作的开展，牵头部门负责按照决策机构议定的工作目标和要求开展数据分类分级工作，牵头制定企业数据分类分级管理办法、制度、流程、标准规范，协调解决分类分级工作中的问题，牵头进行数据分类分级工作的评价。

c） 数据分类分级的实施部门，实施部门负责本部门数据分类分级的具体实施工作，具体包括：按照牵头部门制定的制度、流程、规范等梳理本部门的数据资源，并提交给牵头部门。实施部门包括企业各业务部门和技术部门，业务部门包括人力资源、战略规划、采购、财务、市场、政企、客服等支撑企业运转的部门，技术部门包括企业IT部门、网络部门、业务运营部门等直接参与网络与业务系统建设及业务运营的部门。

7.2 全面梳理数据资源

牵头部门牵头全面梳理企业内部的所有数据资源，业务部门和技术部门配合数据梳理工作，梳理的内容包括以物理或电子形式记录的数据表、数据项、数据文件等，明确数据梳理的要求，包括数据内容描述、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等内容。

7.3 收集整理全部数据资源

对每个部门的所有数据资源进行逻辑汇聚，对所有部门的数据集合，进行合并然后统一列表，形成数据资源列表。

7.4 对数据资源分类

根据基础电信企业业务运营和企业自身管理特点，按照树形结构，建立数据资源分类目录树。并将整理后的数据资源列表对应到目录树，确定数据资源列表中每个数据项在目录树中所在的位置，即确定该数据项的数据类型。

7.5 对数据资源分级

根据基础电信企业数据重要程度和敏感程度，确定数据资源的安全等级。

7.6 数据分类分级标识

基础电信企业应根据数据分类分级方法，采用人工与技术手段相结合的方法，实现企业数据资源的梳理与分类分级，并进行数据分类分级标识。数据分类分级及标识方法建议参见附录C。

7.7 建立数据分类分级清单

根据数据分类分级情况对企业数据资源进行分类分级标识后，输出企业的数据分类分级清单。清单内容至少包括所属部门、所在系统、数据类型、安全等级、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等。

企业建设必要的网络数据资源清单管理技术手段，确保网络数据资源清单内容覆盖全面、信息真实完整。

7.8 实施数据分类分级安全管控

基础电信企业应当根据网络数据资源的分类分级情况，在数据生命周期的各个环节配套差异化的安全保护措施，除满足《YD/T 3802 电信网和互联网数据安全通用要求》外，还应遵循如下管控要点：

a) 基础电信企业应根据本企业数据分类分级管理制度对数据进行分类分级标识。对于在数据库中存储的高安全级别数据（如第4级、第3级数据），标记应细化至数据库表的字段级，其他级别数据采用的标记宜细化到数据库表的字段级。若出现任何没有分级标识的数据，其默认安全控制等级为最高安全等级。

b) 原则上未经过脱敏处理的数据不可降级使用，若确有需要，应执行严格的授权审批流程，并对降级使用数据进行全过程审计。数据使用完毕后，恢复至原安全级别。

c) 数据传输过程中，若涉及高安全级别数据（如第4级、第3级数据）应对数据报文进行加密，并采取措施（如数字签名、MAC等），以保证数据传输的机密性和完整性。

d) 在使用数据或披露前，涉及高安全级别数据的，应采用数据脱敏技术，确保数据使用、对外披露等场景的脱敏。

e) 对于个人敏感信息的安全管控，还应满足GB/T 35273中对个人敏感信息的安全管控要求。

8 数据分类分级方法

8.1 基础电信企业数据分类方法

数据分类按照 GB/T 10113 中的线分类法为基础进行分类。

根据基础电信企业业务运营特点和企业内部管理方法,收集企业内所有部门的数据资源，梳理所有数据资源。按照线分类法，按照业务属性（或特征），将基础电信企业数据分为若干数据大类，然后按照大类内部的数据隶属逻辑关系，将每个大类的数据分为若干层级，每个层级分为若干子类，同一分支的同层级子类之间构成并列关系，不同层级子类之间构成隶属关系。所有数据类及数据子类构成数据资源目录树，如图 1 所示。目录树的所有叶子节点是最小数据类。最小数据类是指属性（或特征）相同或相似的一组数据。

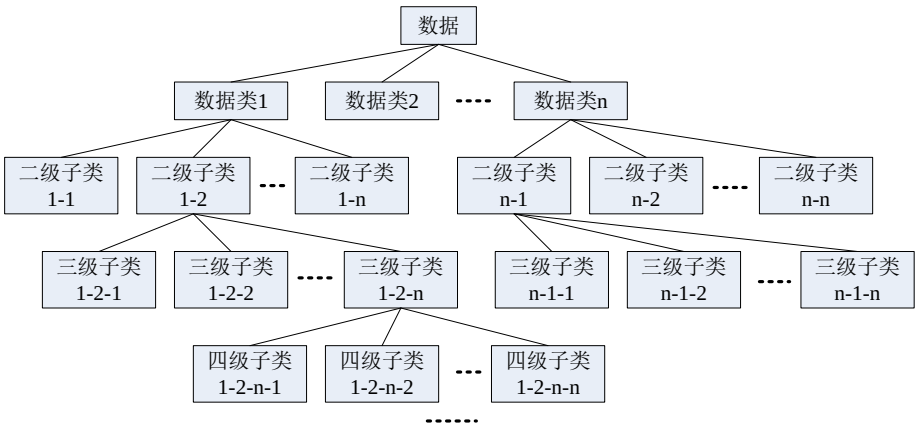

图 1　数据资源分类分级目录树

为便于对数据进行统一管理及应用，根据基础电信企业生产经营管理现状和企业自身管理特点，将基础电信企业掌握的数据整合纳入两大类：

- 用户相关数据，是指与个人用户、集团客户相关的身份相关数据、服务内容数据、用户服务衍生数据等。
- 企业自身数据，是指基础电信企业掌握的与用户无关的数据，包括网络与系统类数据、企业管理类数据、合作伙伴数据等。网络与系统类数据，主要涉及网络与系统的建设与运行维护信息、软硬件资源信息、安全管理信息等数据；企业管理类数据，主要涉及企业战略、规划建设、经营分析、办公自动化等相关数据。

具体分类参见附录A。

其他业务涉及的数据如物联网业务、人工智能业务、云服务业务、移动互联网业务数据的分类不在本标准规定范围。

基础电信企业可根据本单位业务特点，在以上分类的基础上，制定数据分类实施细则，合理进行数据分类，并根据不同类别特点开展数据保护工作。

8.2 基础电信企业数据分级方法

在数据分类基础上,根据基础电信企业数据重要程度以及泄露后对国家安全、社会秩序、企业经营管理和公众利益造成的影响和危害程度，对基础电信企业网络数据资源进行分级。数据分级按照图2所示的步骤和方法进行，具体步骤如下：

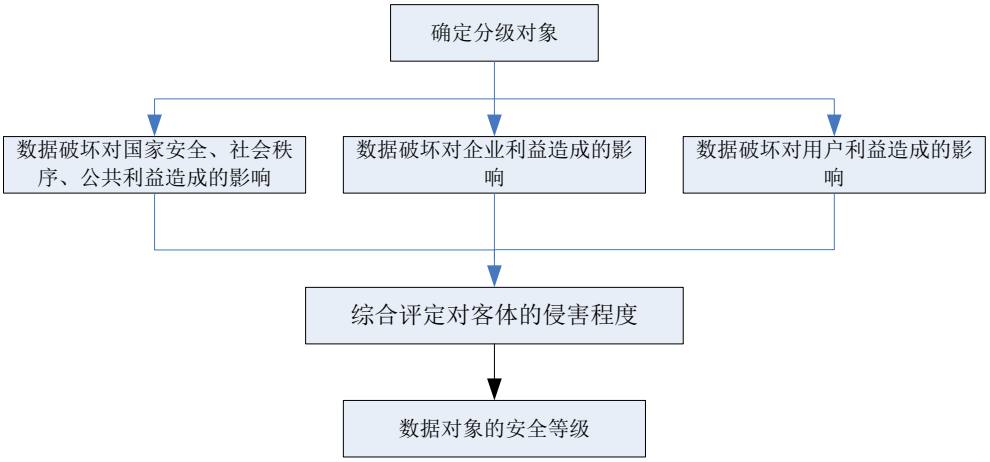

图2 数据分级流程

a） 确定数据分级对象

基础电信企业数据分级对象可以是最小数据类，也可以是最小数据类下的具体数据字段。

b） 确定数据安全受到破坏时造成影响的客体

数据的安全属性（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、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。

根据以上分级因素，形成分级影响程度参照表，如表1所示。

表1 数据分级影响程度参照表

影响类别	影响程度判定原则	影响程度
国家安全和社会公共利益的影响	对国家安全和社会公共利益构成特别严重威胁。数据涵盖范围涉及全国。	严重
	对国家安全和社会公共利益构成严重威胁。数据涵盖范围涉及多省市。	高
	对国家安全和社会公共利益造成较严重威胁。数据涵盖省市。	中
	对国家安全和社会公共利益造成一定影响。	低
企业业务、财务、声誉等影响	导致全部业务无法开展，造成特别严重经济损失，或对全国大量用户产生负面影响；对企业利益和声誉构成特别严重威胁、对用户信任度造成特别严重影响。	严重
	导致部分业务无法开展，造成严重经济损失，或对多省用户产生负面影响；对企业利益和声誉构成严重威胁、对用户信任度造成严重影响。	高
	导致个别业务短时无法开展，造成一定程度的经济损失，或对某地市用户产生负面影响。对企业利益和声誉构成一定程度威胁、造成一定程度影响，对用户信任度造成一定程度影响。	中
	造成轻微经济损失，不影响业务稳定。	低
用户利益影响	用户可能会遭受重大的，不可消除的，可能无法克服的影响。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等。	严重
	用户可能遭受重大影响，克服难度高，消除影响代价大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等。	高
	用户可能会遭受较严重的困扰，且克服困扰存在一定的难度。如付出额外成本、无法使用应提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等。	中
	用户可能会遭受一定程度的困扰，但尚可以克服。如被占用额外的时间、被打扰、产生厌烦和恼怒情绪等。	低

c） 评定对影响客体的影响程度

将分级对象对照数据分级影响程度参照表进行映射，判断分级对象发生丢失、泄露、被篡改、被损毁等安全事件时对影响客体的侵害程度。

d） 确定数据分级对象的安全等级

根据数据对象对客体的影响程度，取影响程度中的最高影响等级为该数据对象的重要敏感程度。例如：若某数据对象发生安全事件时对国家安全和社会公共利益的影响程度为低，对企业利益影响程度为低，对用户利益影响程度为高，则该数据对象的重要敏感程度取三者中最高，即为高。

按照数据对象的重要敏感程度，可以将基础电信企业网络数据资源分为四个安全级别，其对应的安全要求逐级递减，分别为第四级、第三级、第二级和第一级。

第四级数据：一旦丢失、泄露、被篡改、被损毁会对国家安全、社会公共利益或企业利益或用户利益造成特别严重影响的数据，安全管控要求最高；

第三级数据：一旦丢失、泄露、被篡改、被损毁会对国家安全、社会公共利益或企业利益或用户利益造成严重影响的数据，应实施较强的安全管控；

第二级数据：一旦丢失、泄露、被篡改、被损毁会对国家安全、社会公共利益或企业利益或用户利益造成一定程度影响的数据，执行基本的安全管控；

第一级数据：一旦丢失、泄露、被篡改、被损毁对国家安全、社会公共利益或企业利益或用户利益造成影响较小或无影响的数据，对安全管控不作要求。

附录B给出了基础电信企业数据安全分级示例。

企业若在执行四级安全管控落地实施中有难度，可以视实际情况对相邻级别进行合并，实施三级分级方式和相应安全管控措施。

附 录 A

（资料性附录）

基础电信企业数据分类示例

根据基础电信企业业务运营管理和数据安全管理特点，将企业数据分为用户相关数据和企业自身相关数据两大类，表A.1和A.2分别给出了这两大类数据的详细分类示例。

表A.1 用户相关数据分类示例表

1、 用户相关数据		
1-1 用户身份相关数据		
子类	**范围**	**对应数据**
1-1-1 用户身份相关数据	1-1-1-1 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、客户实体编号、集团客户编号、集团客户名称等
	1-1-1-2 网络身份标识	联系电话、邮箱地址、网络客户编号、即时通信账号、网络社交用户账号等
	1-1-1-3 用户基本资料	客户职业、工作单位、居住地址、年龄、性别、籍贯、兴趣爱好等； 集团客户所在省市、所在行业等
	1-1-1-4 实体身份证明	身份证、护照、驾照、营业执照等证件影印件； 指纹、声纹、虹膜等
	1-1-1-5 用户私密资料	揭示个人种族、家属信息、宗教信仰、个人健康、私人生活等用户私密信息； 《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
1-1-2 用户网络身份鉴权信息	1-1-2-1 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，以及与密码关联的密码保护答案等
1-2 用户服务内容数据		
1-2-1 服务内容和资料数据	1-2-1-1 服务内容数据	**1-2-1-1-1 电信网服务内容数据：**短信、彩信、话音等通信内容数据信息； **1-2-1-1-2 移动互联网服务内容信息：**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
	1-2-1-2 联系人信息	用户通讯录、好友列表、群组列表等用户资料数据
1-3 用户服务衍生数据		

1-3-1 用户服务使用数据	1-3-1-1 业务订购关系	**1-3-1-1-1 基本业务订购关系：**品牌、套餐定制等情况； **1-3-1-1-2 增值业务订购关系：**邮箱、通讯录等增值业务的注册、修改、注销等
	1-3-1-2 服务记录和日志	**1-3-1-2-1 服务详单：**语音、短信、彩信和数据详单等； **1-3-1-2-2 移动互联网服务记录：**Cookie 内容、上网日志等
	1-3-1-3 消费信息和账单	**1-3-1-3-1 消费信息：**停开机、入网时间、在网时间、积分、预存款、信用等级等； **1-3-1-3-2 账单：**每月出账的固定费用、通信费用等
	1-3-1-4 位置数据	**1-3-1-4-1 精确位置信息：**小区代码、基站号、基站经纬度坐标等； **1-3-1-4-2 大致位置信息：**地区代码、城市代码等
	1-3-1-5 违规记录数据	**1-3-1-5-1 用户违规记录；**垃圾短信、骚扰电话等相关的黑名单、灰名单等； **1-3-1-5-2 业务违规记录；**端口滥用、违规渠道、不良网站域名等记录及相关黑名单、灰名单等
1-3-2 设备信息	1-3-2-1 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
	1-3-2-2 终端设备资料	终端型号、品牌、厂商等
1-4 用户统计分析类数据		
1-4-1 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。
1-4-2 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

表 A.2 企业自身相关数据分类示例表

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（分发布前后）	2-1-1-1 网络规划类	网络建设数据、网络规划数据等
	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 网络与系统运维类数据	2-1-3-1 信令	信令数据
	2-1-3-2 路由信息	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	时间、地点、事件、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	网络及系统的运行统计分析数据等

	统计分析	
2-1-4 网络安全管理类数据	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	违法有害信息监测处置、舆情态势监测预警等数据
	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 安全事件记录等信息
2-2 业务运营类数据		
2-2-1 业务运营服务数据	2-2-1-1 产品信息	产品 ID、套餐设置、销售品 ID 等
	2-2-1-2 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
	2-2-1-3 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
	2-2-1-4 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
2-2-2 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
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
2-3-2 业务发展类	2-3-2-1 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
	2-3-2-2 营销管理	品牌及传播推广策略、业务发展策略、管理办法、等
	2-3-2-3 资费管理	资费方案、资费管理等信息

	2-3-2-4 产品发展策略	产品试点方案、试商用方案、业务融合方案等
2-3-3 技术研发类	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
2-3-4 运行管理类		运行管理相关的规程、操作指南、计划等
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	信息披露相关材料、业绩披露信息等
	2-3-5-3 考核相关信息	经营业绩考核办法等信息
	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
2-3-6 综合管理类	2-3-6-1 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
	2-3-6-2 财务信息	收入、利润、预算、决算数据等
	2-3-6-3 办公自动化	邮件、行政文件、签报等信息
	2-3-6-4 采购	**2-3-6-4-1 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 **2-3-6-4-2 物资数据：**采购物资数量、类型等信息 **2-3-6-4-3 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
2-4 其他数据		
2-4-1 合作方提供数据		音视频等互联网内容数据

附 录 B
（资料性附录）
基础电信企业数据分级示例

按照数据对象的重要敏感程度，将基础电信企业网络数据资源分为四个安全级别，各个安全级别包含的数据子类示例如表 B.1 所示。

表 B.1 数据分级示例表

类别	子类
第四级	1-1-1-4 实体身份证明、1-1-1-5 用户私密资料、1-1-2-1 用户密码及关联信息、1-2-1-1 服务内容数据、1-2-1-2 联系人信息、2-1-1 规划建设类数据（发布前）、2-1-2 网络与系统资源类数据、2-1-3 网络与系统运维类数据、2-1-4 网络安全管理类数据
第三级	1-1-1-1 自然人身份标识、1-3-1-2 服务记录和日志、1-3-1-4-1 精确位置信息、1-4-1 用户使用习惯和行为分析数据、1-4-2 用户上网行为相关统计分析数据 2-3-1 发展战略与重大决策、2-3-2 业务发展类、2-3-3 技术研发类、2-3-5 生产经营类、2-3-6-4-1 招投标数据（公开前）
第二级	1-1-1-2 网络身份标识、1-1-1-3 用户基本资料、1-3-2-1 设备信息、1-3-1-1 业务订购关系、1-3-1-3-1 消费信息、1-3-1-3-2 账单、1-3-1-4-2 大致位置信息 2-1-1 规划建设类数据（发布后）、2-2-1-2 渠道信息、2-2-1-3 客户服务信息、2-2-1-4 营销信息 2-3-6-4-1 招投标数据（公开后）、2-3-6-4-2 物资数据、2-3-6-4-3 业务合作类数据、2-4-1 合作方提供数据
第一级	1-3-1-5 违规记录数据 2-2-1-1 产品信息、2-2-2 公开业务运营服务数据

附 录 C
（资料性附录）
基础电信企业数据分类分级标识方法

自动化数据分类分级标识过程可以通过如下五个环节完成。

C.1 制定企业数据分类分级策略

企业通过参考数据分类分级相关的国家、行业标准以及企业自身的管理制度制定符合企业自身数据特点和数据安全管理要求的数据分类分级保护策略，制定出数据分类目录。

C.2 定义数据模型

根据企业数据分类分级的策略，针对不同类型、不同级别的数据的特点，定义数据模型。数据模型可以通过如下几种方式定义：

a) 关键字、正则表达式等形式，实现邮箱、身份证号、银行账号、电话号码等明显特征数据的建模。

b) 数据指纹技术，实现对批量数据的指纹索引化处理。

c) 机器学习算法，实现对大批量数据的训练后的建模分析，此种数据模型定义方式需要提供批量的敏感数据样本数据供建模分析。

C.3 分类分级策略与数据模型关联

参考企业数据分类分级保护策略将数据模型划归至不同的数据类别与数据级别，即将数据与数据分类、数据分级策略建立关联，以支持后续的数据自动化分类分级。

C.4 利用工具对目标数据资源自动化识别

结构化数据和非结构化数据的自动化识别方式如下：

a) 结构化数据识别：

1) 利用可控权限账号，接入数据库，通过查询指令结合数据安全模型，进行结构化数据自动化静态识别。

2) 识别数据库协议并解析流量数据，通过数据安全模型结合特征分析和机器学习，进行结构化自动化数据动态识别。

3) 梳理业务流，通过特征分析和机器学习分析业务会话，进行结构化自动化数据动态识别。

b) 非结构化数据识别：

1) 对接应用服务器、文件管理服务器等，利用全文检索技术，通过 NLP、数据清洗和机器学习（可结合大数据分析技术），实现文本数据识别；

2) 对接（通信协议、网络爬虫等）应用服务器、文件管理服务器等，利用属性识别技术，通过图像识别和机器学习，实现图像数据识别；

3） 对接（通信协议、网络爬虫等）应用服务器、文件管理服务器，利用属性识别技术，通过语音识别和机器学习，实现语音数据自动化识别；

4） 建立大数据分析技术，对企业源数据进行整合，实现有监督和无监督机器学习，以实现海量数据动态识别。

C.5 数据分类分级索引标识

通过自动化数据分类分级工具扫描发现不同数据类型、不同数据级别的数据之后，给这些数据按照分类分级策略进行索引标识，标记数据项的类别和级别，以便后续数据安全防护过程中匹配不同类型、不同级别的安全防护措施。