

信托公司数据分类分级实施指南

(2026年9月17日经中国信托业协会第46次会员大会审议通过)

第一章 总则

第一条 **【整体工作背景】**为规范信托行业数据处理活动，保障数据安全、金融安全，构建贯穿数据生命周期全过程的数据分类分级管理体系，精准识别并有效保护信托行业核心数据资源，促进数据合理开发利用，系统性提升信托公司数据安全治理能力与安全保障水平，保护个人、组织的合法权益，服务金融高质量发展，维护国家安全和社会公共利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》《网络数据安全条例》《银行保险机构数据安全管理办法》等法律、行政法规及行业规章，制定本指南。

第二条 **【分类分级目标】**数据分类分级旨在对本机构数据资源进行全面梳理，明确数据资源所属类别和级别，以确立适当的数据分类分级保护体系和保护措施，促进数据合法合规开发利用。加快推动并完成本机构数据分类分级工作，是信托公司开展全域数据资产登记管理、建立健全自身数据安全管理制度、构建覆盖数据全生命周期和应用场景的安全

保护机制，并逐步形成与本机构业务发展目标相适应的数据安全治理体系的基础工作，也是持续提升信托行业整体数据安全保障能力和金融领域数据要素高水平应用的必要前提。

第三条 【基本工作规范】信托公司应当依据国家与行业监管部门法律、行政法规、行业规章及标准规范等要求，制定本机构数据分类分级保护制度，建立数据目录及分类分级规范，动态管理和维护数据目录，配套落地差异化的数据安全管控机制，推动实施数据分类分级保护。信托公司数据分类分级结果应当经本机构内部评审及批准后，形成本机构数据目录。

【重要数据目录】信托公司应当在本行业监管部门的监督指导下，向国家金融监督管理总局或者其派出机构报送本机构重要数据目录。信托公司重要数据目录发生重大变化应当及时报备更新后的数据目录。

第四条 【基本原则】数据分类分级是数据安全与治理的核心基础工作，其工作要求和工作规程应当围绕“依法合规、全面覆盖、风险导向、科学实用、动态调整、权责一致”六大核心原则构建，旨在实现对不同来源、不同用途、不同价值、不同风险的数据进行差异化管理，形成兼具科学性、适用性和可操作性的分类分级体系。

（一）依法合规原则

数据分类分级应当严格遵循国家及行业数据安全相关法律、行政法规及行业规章的有关规定，确保分类分级的制度、方法、流程及结果的合规性和合理性。

(二) 全面覆盖原则

数据分类分级应当涵盖信托公司全量数据资源，覆盖收集、存储、使用、加工、传输、提供、共享、转移、公开、删除、销毁等数据全生命周期各环节的各类数据处理活动，确保数据资产安全管理工作无遗漏、无死角。

(三) 风险导向原则

数据分类分级应当考虑数据的泄露、篡改、损毁或者非法获取、非法使用、非法共享等潜在风险，综合评估对国家安全、公共利益、个人及组织权益的危害程度，以风险防控为核心制定分类分级规则，优先保障高敏感、高价值数据的安全性。

(四) 科学实用原则

数据分类分级应当立足信托业务实际场景，结合数据应用需求与固有属性特征，构建具备科学性和可操作性的分类分级规范和操作规程，切实保障数据的安全有序利用。

(五) 动态调整原则

数据分类分级应当根据业务模式变化、监管政策更新及

技术发展等情况，定期对数据分类分级结果进行复审，及时调整级别，确保分类分级工作过程及工作结果始终与实际数据安全管理及数据有效利用的总体目标相匹配。

（六）权责一致原则

数据分类分级应当明确董事会、管理部门、业务部门、技术部门及相关人员岗位的职责分工以及内部协同合作机制，建立覆盖决策、管理、实施、监督的闭环管理体系，确保管理权责明确、责任到岗到人，切实保障分类分级工作有效落地。

第二章 适用范围

第五条 【机构范围】本指南所称信托公司，是指依照《中华人民共和国公司法》和《信托公司管理办法》在中华人民共和国境内设立的主要经营信托业务的金融机构。

第六条 【数据范围】信托公司应当对其开展业务及经营管理过程中获取、产生的数据进行分类分级管理。其中，未经电子化的数据，应当依据档案文件等有关管理规范执行；涉及国家秘密的数据，应当依据国家有关法律法规执行。

第七条 【例外情况】开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。国家有关主管部门另有规定的，应当依法遵守

其规定。

第三章 工作保障

第八条 **【组织架构】**信托公司应当结合本机构管理架构和运营体系实际情况，依据“谁管业务、谁管业务数据、谁管数据安全”原则，建立覆盖党委（党组）、董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构，明确岗位职责和工作机制，建立健全数据分类分级工作责任体系，为数据分类分级工作构建可靠的组织保障。

（一）建立自上而下的穿透式治理架构。信托公司应当构建“党委（党组）统筹引领、董（理）事会战略决策、经营管理层具体执行、部门协同落实、岗位精准履职”的五级责任体系，形成横向到边、纵向到底的数据安全治理闭环。建设过程中，信托公司应当明确党委（党组）对数据安全的全面领导责任，董（理）事会主导审定数据安全战略规划与核心制度，机构主要负责人履行数据安全管理工作第一责任人职责，分管领导负直接责任并牵头制定数据安全管理工作落地细则，同时，应当将责任节点嵌入本机构全业务流程，通过常态化督查、闭环考核与问责机制，确保数据安全治理要求深度穿透至各业务条线与基层岗位。

（二）明确归口管理部门及其职能。信托公司应当指定本

机构数据安全归口管理部门，作为本机构负责数据安全工作的主责部门，并负责牵头组织和督促数据资产安全管理、数据安全管理制度建设、数据安全防护机制构建等日常管理工作的执行。数据安全归口管理部门应当主导制定分类分级相关制度和流程，组织开展数据目录的建立、维护、定期审核和动态调整等工作，并协调跨部门资源，确保分类分级与业务场景紧密衔接。

(三)建立业务与技术协同机制。信托公司数据安全归口管理部门应当组织制定分类分级相关工作流程及操作规程，并指定本机构分类分级工作牵头部门，由其负责组织和落实本机构数据分类分级工作。其中，本机构业务部门应当承担具体业务数据的管理职责，基于业务属性定义分类维度，判定数据分类分级结果并提出数据安全保护需求。本机构技术部门应当提供技术和工具能力支持，负责落地实施数据的分类分级标记、识别及相关管理规程。本机构风险管理与内控部门应当负责审计和监督数据分类分级全过程执行情况。

第九条 【制度规程】信托公司应当在国家及行业监管部门监督指导下，结合本机构总体数据安全管理策略和规划，建立数据分类分级相应管理制度和操作规程，确保数据分类分级工作落实法律、行政法规及行业规章相关规定，并切实保障数据分类分级落地实施工作的稳妥有序开展。

(一)明确数据安全策略和规划。信托公司应当理清数据安全工作的总体策略、方针、目标，形成数据安全工作方向和计划，并据此制定涵盖数据资源识别、数据分类分级及其标记、数据目录建立与维护等工作事项的数据安全管理总体要求和工作任务，建立健全跨部门配合机制及相关资源支持体系。同时将数据安全纳入本机构全面风险管理体系，定期评估数据安全策略和机制的有效性。

(二)制定数据分类分级制度规程。信托公司应当有效规范数据分类分级规则、方法、标准和流程等工作细则，明确数据分类分级工作策略、具体要求、实施方案、涉及的角色及其职责、数据目录建立及其审核修订要求、人员操作规程、审批流程、分类分级变更规则和机制，以及相关制度规程的制定、发布、维护和更新机制等工作要求。

(三)建立数据目录管理机制。信托公司应当形成常态化的数据目录管理能力，规范数据目录制定、审议、发布、变更和维护流程，明确数据目录管理统筹方和参与方，建立并动态维护本机构数据资源模板及数据目录。涉及重要数据的，信托机构应当按照国家及行业监管部门的工作要求，及时开展重要数据的识别认定和报送工作。

第四章 工作方法

第十条 数据分类

（一）类别描述

信托公司应当对本机构开展业务及经营管理过程中获取、产生的数据进行分类。数据类型包括但不限于客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。相关数据类别定义如下：

1. 一级分类

客户数据：服务对象的自然属性和金融身份识别数据；

业务数据：在提供金融服务过程中产生的数据；

经营管理数据：履行职能与经营管理过程中产生、记录的数据；

系统运行和安全管理数据：信息系统及其相关信息基础设施建设和运行过程中产生的数据。

2. 二级分类

信托客户（自然人）：指信托业务中自然人委托人及受益人的相关要素信息；

信托客户（机构）：指信托业务中机构委托人及受益人的相关要素信息；

信托客户（金融产品）：指信托业务中作为委托人或受益人的金融产品相关信息；

交易对手信息：指信托业务开展过程中涉及的各类交易对手方的要素信息；

信托业务：指信托公司开展的信托业务相关信息；

信托会计信息：指信托公司信托财产相关的财务核算与披露信息；

固有业务：指信托公司运用自有资金开展的业务相关信息；

固有会计信息：指信托公司自有资金相关的财务核算与披露信息；

战略管理数据：涵盖公司长期发展规划、市场定位、竞争分析及业务拓展策略等关键决策信息；

人力资源管理数据：涵盖员工全生命周期（入职至离职）的招聘、合同薪酬、绩效培训、考勤休假及员工关系等信息；

财务管理数据：涵盖会计记录、预算编制、成本控制、税务资金运作及反映企业财务状况的各类信息；

风险管理数据：指用于识别、评估、监控和控制企业各类风险的关键信息；

法律事务管理数据：涵盖合同管理、诉讼仲裁、合规审查、法律风险评估及监管报送相关的法律记录；

纪检审计管理数据：指党内监督及企业内部审计过程中收集的各类监督信息；

综合行政管理数据：涵盖党建、公文、品牌、董办、工会、外事及日常办公管理等运营信息；

监督管理数据：指监管机构下发指令及公司上报监管的相关数据；

规划研发数据：指 IT 规划及系统研发过程中涉及的技术与管理信息；

系统运维数据：指信息技术基础设施、系统运行维护及信息安全相关的管理记录。

(二) 分类方法

信托公司应当根据数据管理和数据使用需求，结合本机构已有数据治理工作基础，综合考虑以下属性对数据进行细化分类：

1. 数据所涉业务属性，即按照业务范围、业务种类或者业务功能进行分类，如资产服务、资产管理等；
2. 数据所涉责任部门，即按照数据管理部门或者职责分工进行细化分类；
3. 数据所涉描述对象，即按照数据描述的对象进行细化分类，如业务数据、经营管理数据等；

4. 数据所涉流程环节，即按照业务流程、产业链环节进行细化分类；
5. 数据所涉来源方式，即按照数据来源、收集方式进行细化分类，如内部产生、外部获取等；
6. 数据所涉主体特征，即按照数据主体或者属主进行细化分类，如公共数据、组织数据、个人信息等。

其中，数据资产中如涉及法律法规有专门管理要求的数据类别（如个人信息等），应当按照有关法律法规的规定及相关标准规范进行识别和分类。

（三）分类规则

信托公司应当根据行业监管部门有关规定，综合考虑数据所涉业务属性以及数据所涉描述对象特性，从客户数据、业务数据、经营管理数据、系统运行和安全管理数据等维度识别和确定本机构数据资产的基础类别。

客户数据是指在开展业务服务过程中从个人客户或者组织客户收集的数据，以及在业务服务过程中产生的归属于客户的数据，包括但不限于个人信息、组织客户信息等。

业务数据是指在业务的研发、生产、运营过程中收集和产生的非客户类数据，包括但不限于信托产品数据、合同协议等。

经营管理数据是指在本机构经营和内部管理过程中收集和产生的数据，包括但不限于经营战略、财务数据、人力资源管理数据、市场营销数据等。

系统运行和安全管理数据是指网络和信息系統运行维护、日志记录及网络安全数据，包括但不限于网络设备和信息系统的配置数据、日志数据、安全监测数据、安全漏洞数据、安全事件数据等。

在此基础上，信托公司应当结合自身实际情况，灵活选用与本机构数据管理与使用需求相适应的分类属性，对基础类别进行进一步的逐层细化分类，进而构建层层隶属、由总到分的数据分类体系。

第十一条 数据分级

(一) 级别描述

信托公司应当根据数据的重要性和敏感程度，将数据级别从高到低分为核心数据、重要数据、一般数据，参见表 4.1。其中，一般数据细分为敏感数据和其他一般数据。

表 4.1 数据分级及级别描述

数据级别		级别描述
核心数据		指对领域、群体、区域具有较高覆盖度或者达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或者共享，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。
重要数据		指特定领域、特定群体、特定区域或者达到一定精度和规模的数据，一旦被泄露或者篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。
一般数据	敏感数据	指一旦被泄露或者篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或者对组织自身或者公民个体造成重要影响的数据。
	其他一般数据	指除以上数据之外的其他数据。

(二) 分级方法

信托公司应当通过开展数据安全影响分析的方式进行数据级别的分析和识别，参见表 4.2，其中：

影响对象是指潜在的数据安全风险或者可能发生的数据安全事件，可能会对其产生不良影响的主要危害对象。其中，数据安全风险主要考虑本机构业务和系统运行及各类数据处理活动中存在的可能造成泄露、篡改、损毁或者非法获取、非法使用、非法共享等数据安全问题的威胁和隐患。影响对象通常包括国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益。

影响程度是指数据一旦遭到泄露、篡改、损毁或者非法

获取、非法使用、非法共享等威胁和攻击，可能造成不良后果及其危害的严重程度。影响程度从高到低可分为特别严重危害、严重危害、一般危害。

表 4.2 数据影响分析方法示例

影响对象	分析方法描述	
	国家安全	例如影响国家政治、国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等国家利益安全。
	经济运行	例如影响市场经济运行秩序、宏观经济形势、国民经济命脉、行业领域产业发展等经济运行机制。
	社会秩序	例如影响社会治安和公共安全、社会日常生活秩序、民生福祉、法治和伦理道德等社会秩序。
	公共利益	例如影响社会公众使用公共服务、公共设施、公共资源或者影响公共健康安全等公共利益。
	组织权益	例如影响组织自身或者其他组织的生产运营、声誉形象、公信力、知识产权等组织权益。
	个人权益	例如影响自然人的的人身权、财产权、隐私权、个人信息权益等个人权益。
影响程度	特别严重危害	1. 可能导致危及国家安全的重大事件，发生危害国家利益或者造成重大损失的情况； 2. 可能导致严重危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致金融市场秩序遭到严重破坏等情况； 3. 可能导致金融业态机构遭到监管部门严重处罚，或者影响重要/关键业务无法正常开展的情况； 4. 可能导致重大个人信息安全风险、侵犯个人隐私等严重危害个人权益的事件。
		例如：直接影响政治安全、关系国民经济命脉、重要民生、重大公共利益、超大规模个人或者组织权益的，应将影响程度确定为特别严重

		危害。
	严重危害	1. 可能导致危害社会秩序和公共利益的事件，引发区域性集体诉讼事件，或者导致金融市场秩序遭到破坏等情况； 2. 可能导致金融业机构遭到监管部门处罚，或者影响部分业务无法正常开展的情况； 3. 可能导致一定规模的个人信息泄露、滥用等安全风险，或者对个人权益可能造成一定影响的事件。
		例如：关系国家安全重点领域，直接危害宏观经济运行、社会稳定、危害公共健康和安全、大规模的个人或者组织权益的，或者对行业领域或者地区的经济发展造成严重危害的，应将影响程度确定为严重危害。
	一般危害	1. 可能导致个别诉讼事件，使金融业机构经济利益、声誉等轻微受损； 2. 可能导致金融业机构部分业务临时性中断等情况； 3. 可能导致超出个人客户授权加工、处理、使用数据等情况，对个人权益造成部分或者潜在影响。
		例如：仅影响小范围个人或者组织权益的，同时评估个人信息规模及是否会对国家安全、经济运行、社会秩序或者公共利益造成影响以及影响程度后，可将影响程度确定为一般危害。

(三) 分级规则

信托公司应当严格遵循国家及行业监管部门有关法律、法规，明确并建立本机构数据级别的分析和识别的工作方法及操作规程，明确数据分级的操作流程、分析方法、认定规则以及审批审核流程等工作要求，数据级别识别规则的构建模式可参见表 4.3。

对于核心数据和重要数据，信托公司应当按国家和行业监管部门有关要求，及时进行相关数据的识别和申报，建立

数据目录，并做好数据目录的日常管理和数据安全保护工作。

对于一般数据，信托公司应当综合考虑影响对象和影响程度进行分析，根据数据在经济社会发展中的重要程度，以及一旦遭到泄漏、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，对敏感数据、其他一般数据进行识别和标识。

表 4.3 数据级别的识别规则示例

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益	一般数据	一般数据	一般数据
个人权益	一般数据	一般数据	一般数据
注：以上规则仅供示例使用，如影响大规模的个人或组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国家安全、经济运行、社会秩序或公共利益造成影响，那么相应数据级别也可能高于一般数据。			

第五章 工作流程

第十二条 【基本流程】信托公司应当明确并建立数据分类分级工作流程，形成本机构统一、规范和标准的工作程序和操作流程，工作流程应至少包含工作准备、资产梳理、数据分类、数据分级、结果审核以及批准应用等环节，可参

见图 5.1。

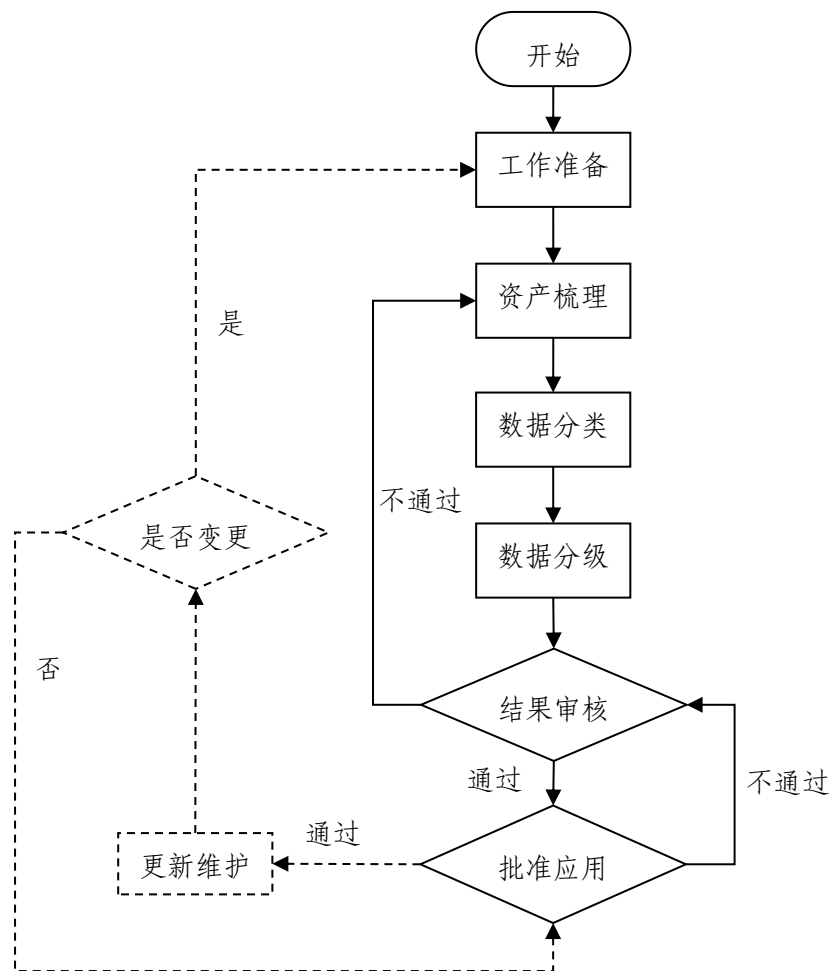


图 5.1 数据分类分级工作流程示意图

第十三条 【工作准备】工作准备环节应当明确数据分类分级的范围和工作目标，明确数据分类分级工作组织、职责分工和协作机制等工作框架、方案和计划，并明确当前数据分类分级的颗粒度（如文件、表、字段等）、适用规则等具体任务的关键细节要求。

第十四条 【资产梳理】资产梳理环节应当对本机构数据进行全面的盘点和梳理，形成统一的数据资源清单，掌握

当前数据的规模、位置 and 状态等基本情况，并进行数据分类分级合规性准备工作。

第十五条 **【数据分类】**数据分类环节应当开展数据属性分析，依据数据分类规则，进行数据类别的分析、识别和判定，形成初步的数据分类结果。

第十六条 **【数据分级】**数据分级环节应当开展数据影响分析，依据数据分级规则，进行数据级别的分析、识别和判定，形成初步的数据分级结果。

第十七条 **【结果审核】**结果审核环节应当对照数据分类分级合规性准备工作情况及本机构数据分类分级规范等制度规程，对初步的数据分类分级结果（信托公司典型数据的分类分级可参见附件）及工作过程进行复核与修正，审核通过的，形成数据分类分级结果；审核不通过的，应重新识别数据资产及相应数据的类别级别。

第十八条 **【批准应用】**批准应用环节应当由本机构数据安全归口管理部门组织并牵头开展数据分类分级过程及结果的审议和批准工作，经本机构数据安全管理工作相关最高责任人或者责任组织审批通过后，确定本机构数据分类分级结果及数据目录；审批不通过的，应重新发起结果审核。

第六章 更新维护

第十九条 信托公司应当加强数据分类分级结果的时效性管理，建立数据目录动态调整与更新机制，数据分类分级结果的更新工作流程可参见图 5.1。当数据的业务架构、重要程度、数据安全风险及一旦出现数据安全问题可能造成的危害程度等发生变化，可能导致原分类分级结果不再适用的，信托公司应当及时审核并动态调整，包括但不限于：

（一）信托公司应当每年按照监管部门相关要求开展重要数据及核心数据识别与目录填报，根据最终认定结果及时更新数据目录。

（二）信托公司业务架构、信息系统、数据规模、数据使用场景、数据加工方式等发生重大变更时，应当及时开展数据分类分级结果的适用性评估，并对新产生的数据或者衍生数据的类别、级别进行识别，据此更新数据目录。

（三）信托公司发生重大或者特别重大数据安全事件后，应当评估对所涉数据敏感性产生的影响，及时调整相应的数据分级结果并更新数据目录。

（四）因国家或者行业监管部门要求，导致原定的数据分类分级结果不再适用时，信托公司应当及时开展数据分类分级规则对标调整工作，重新识别数据类别与级别，完成数据目录更新。

（五）信托公司需要对数据分类分级进行变更的其他情形。

第七章 附则

第二十条 术语解释

(一) **数据**，是指以电子或者其他方式对信息的记录。

(二) **数据处理**，是指对数据的收集、存储、使用、加工、传输、提供、共享、转移、公开、删除、销毁等。

(三) **数据安全**，是指通过采取必要措施，对数据处理活动和数据应用场景进行管理与控制，确保数据始终处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

(四) **数据主体**，是指数据所标识的自然人或者其监护人、企业、机关、事业单位、社会团体和其他组织。

第二十一条 本指南经协会审议通过后生效。

第二十二条 本指南由协会负责修订和解释。

附件：信托公司典型数据的分类分级参考示例

附件：

信托公司典型数据的分类分级参考示例

信托公司典型数据的分类分级参考示例见附件表 1，实际应用过程中，各机构应当根据其数据的类型、特性、规模、机构特性、业务情况等因素，综合考虑本机构数据安全管理的策略和目标，按照适当的维度、颗粒度对本机构数据资产梳理和细分，确定各项数据的类别，并采取“就高从严”原则确定数据级别，建立数据目录。其中，重要数据和核心数据的识别、认定及保护工作，应当严格按照国家和行业监管部门有关规定和要求执行。各层级分类中的“其他 XX 信息”是指尚未被现有类目覆盖、需要进一步识别和归类的数据，信托公司应在数据产生或首次使用时，依据其数据类型、内容特性、使用价值、泄露影响范围等因素，参照现有分级标准进行级别判定。在未完成定级前，该数据应被视为“敏感”级别进行管控。

附件：信托公司典型数据分类分级参考示例（详见配套 Excel 文件）