CAICT 中国信通院

集智 专题报告

移动互联网应用程序（APP）风险分类分级指南

（2025 年）

中国信息通信研究院泰尔终端实验室

中国信息通信研究院技术与标准研究所

2025年6月

版权声明

前　言

当前，数字经济蓬勃发展，信息技术创新日新月异，移动互联网应用程序（APP）作为数字化、网络化、智能化应用的重要载体，在便利人民群众的生产生活，赋能、赋值、赋智千行百业，推动经济社会数字化转型等方面发挥了重要作用。同时，随着 APP 应用场景日益丰富，个人信息收集、使用更为广泛，加强个人信息保护已成为业界高度关注的重要问题之一。我国高度重视个人信息保护，已出台《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》《网络数据安全管理条例》等法律法规，相关行业主管部门持续完善配套制度体系，组织制定一系列国家、行业及团体标准，为产业各方提供明确指引。

相较于其他行业领域，移动互联网产业具有以下特点：一是 APP 数量多、创新能力强，小程序、快应用、H5 页面、AI Agent 等新形态不断涌现；二是版本更新频繁，单个 APP 平均每月更新 2 到 3 次；三是主体多、链条长，覆盖 APP、SDK、安全厂商、移动应用分发平台、智能终端等上下游企业；四是技术对抗性强，恶意开发者利用“热更新”“云控”等技术，绕开审查、逃避监管。这些特性导致追溯责任和定位问题源头极为困难，对 APP 治理中全链条、全流程风险管理提出了更高要求。

APP 治理需持续深化对行业发展规律的洞察，聚焦行业发展中衍生的新问题、用户使用中亟需解决的痛点问题，持续健全完善综合治理体系，筑牢 APP 开发运营、应用分发、终端运行“三道防线”，

督促 APP 企业从源头强化责任意识、提升服务质量，同时发挥应用分发平台、智能终端等主体的重要作用，通过各链条联防共治，共同提高行业整体服务水平。

鉴于此，本报告基于对 APP 风险特征、风险影响对象、风险影响程度等要素的分析，提出 APP 风险分类分级指南。本报告旨在为监管部门、APP、SDK、安全厂商、应用分发平台、智能终端等上下游企业以及用户提供可参考的风险评估框架，促进各方对 APP 风险类别及其危害形成共识，为进一步围绕不同类别和级别的 APP 风险开展协同治理奠定坚实基础。

目 录

表 目 录

一、产业持续健康发展，生态治理稳步推进

（一）产业规模持续增长，多元创新激发产业活力

近年来，我国移动互联网产业展现出强劲的发展活力，整体规模、用户行为、创新应用等方面均发生了深刻变革，成为推动经济社会数字化转型的关键力量。

移动互联网整体产业规模持续增长。2024 年，移动互联网接入流量达 3376 亿 GB，比上年增长 11.6%。截至 2024 年底，移动互联网用户达 15.7 亿户，全年净增 4575 万户；全年移动互联网月户均流量（DOU）达 18.18GB/户月，比上年增长 7.4%。移动互联网在用户覆盖和流量使用上均保持稳定增长步伐，为产业发展奠定了坚实基础。

小程序爆发式增长，成为移动互联网产业中的重要一环。微信小程序于 2017 年正式发布，其即点即用的便捷化方式带动整体规模快速增长，2018 年微信小程序数量已达到 58 万个。研究数据显示，2024 年 12 月，微信、支付宝和抖音的小程序月活跃用户分别达到 9.36 亿、6.85 亿、2.66 亿[1]。小程序以便捷、灵活、轻量等特点，满足了用户在生活、工作、娱乐等方面的多样化需求。

AI 应用呈现快速发展态势。APP 内嵌 AI 插件成为吸引用户的重要形式，大量互联网头部企业迅速接入。在 AI 加持下，APP 用户规模及用户黏性持续增长，研究数据显示，2024 年 12 月，AI 原生 APP 月度活跃用户已经突破 1.2 亿，同比增长 232%，同时，用户粘

[1] 来源：《2024 年全景生态流量年度报告》，QuestMobile

性也持续增长，整体月人均使用时长达 133.0 分钟，月人均使用次数也达到 49.6 次[2]。AI 正在深刻改变移动应用市场的格局，成为推动行业发展的重要力量，伴随智能体生态的逐渐兴起，其未来发展潜力巨大[3]。

（二）监管治理扎实推进，用户权益保护走深向实

工业和信息化部立足行业管理职责定位，标本兼治、综合施策，深入推进 APP 治理，扎实做好用户权益保护工作。

依法治理方面，落实国家法律法规要求，联合中央网信办、公安部、市场监管总局等部门不断健全 APP 监管治理相关制度体系，发布《常见类型移动互联网应用程序必要个人信息范围规定》《互联网弹窗信息推送服务管理规定》《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理暂行办法》等规章制度。先后出台《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》《关于开展信息通信服务感知提升行动的通知》《关于进一步提升移动互联网应用服务能力的通知》等政策文件，为企业开展经营活动提供更加明确的指引。

专项治理方面，自 2019 年以来，纵深推进 APP 侵害用户权益专项整治，组织开展 APP 技术抽测 47 批次，持续整治违规收集个人信息、强制索取权限等侵害用户权益的问题。截至 2025 年 5 月，累计责令整改 10155 款，公开通报 3079 款违规 APP，下架 646 款整改不到位的 APP。经过集中整治，群众普遍反映强烈的弹窗信息关

[2] 来源：《2024 年 AIGC 应用发展年度盘点》，QuestMobile
[3] 来源：QuestMobile《2025 中国移动互联网春季报告》

闭按钮“小如蝼蚁” “摇一摇”乱跳转、“不下载不让看全文”等突出问题得到有效规范，APP 使用体验更清爽、更顺畅、更便捷。

科技治理方面，组织建设了“面向移动互联网应用程序的检测及认证公共服务平台”，与国内主流移动应用分发平台建立了数据采集机制，实现对 APP 上架数量、下载量、活跃度等情况的动态监测，具备在架 APP 检测全覆盖能力，大幅提升 APP 监测检测、溯源追踪、风险预警、信息共享等技术能力。建立全国 SDK 管理服务平台信息库，覆盖行业 80%的主流产品，有效指引 APP 开发者对比选择 SDK 产品。组织研制发布“智御”个人信息保护人工智能大模型，构建 AI 赋能 APP 合规新范式。

系统治理方面，压实 APP、SDK、应用分发平台、智能终端等上下游企业主体责任。指导重点 APP 企业成立用户权益保护负责部门，建立健全管理制度，开发部署技术手段，加强人员教育培训。督促移动应用分发平台发挥“守门员”作用，细化 APP 上架审核标准，提升 APP 风险检测能力，强化在架 APP 巡查力度。推动主流 SDK 落实最小必要原则，提供个人信息收集的配置选项。推动手机终端厂商对调用位置、摄像头、麦克风等敏感权限进行提醒，强化 APP 运行管理和风险防护，共同营造健康服务环境。

（三）行业协作持续深化，多措并举促进规范发展

科研院所、行业协会等多方力量积极发挥自身优势，通过制定标准规范、强化技术推广、促进行业自律等助力行业健康有序发展。

标准规范方面，中国信息通信研究院联合全国网络安全标准化

技术委员会、中国通信标准化协会、电信终端产业协会等标准化组织，制定《信息安全技术 移动智能终端安全技术要求和测试评价方法》《移动应用分发平台 服务管理要求》《APP 用户权益保护测评规范》等系列标准，形成 12 项国标、90 项行标、191 项团标的标准体系，为企业理解政策法规、加强技术成果应用提供重要参考。

技术推广方面，工业和信息化部移动应用创新与治理技术重点实验室围绕匿名化、隐私计算等关键技术应用，聚焦热更新、生成式人工智能服务、智能网联汽车个人信息保护等产业热点问题开展开放课题研究，组织召开“凝智前行”系列研讨交流会，促进产学研之间的技术交流及推广应用。

行业自律方面，通过公益培训宣讲、优秀案例征集、发布自律公约等活动，加强法律法规宣贯解读，推广典型经验做法，增进各方交流互动，引导创建规范有序的行业生态。如，电信终端产业协会组织发布《移动应用软件高 API 等级预置与分发自律公约》，推动国内预置和上架应用的 targetSdkVersion（Android API 等级）达到 30 级以上，应用生态全面升级转向安卓 11 及以上版本，全面提高移动智能终端及应用安全水平。

二、应用创新蕴含风险，安全治理应对挑战

数字经济时代，移动互联网领域创新活跃，各类新技术新应用不断涌现，为用户带来更加便捷、智能、个性化的服务体验，但也加剧了违规行为的隐匿性、多变性，引发一系列亟待解决的难题。

（一）APP 衍生形态多样，责任界定难度加大

便捷化移动互联网应用快速迭代，不断催生 Hybrid App、快应用、小程序、应用 SDK、WAP 站、Web 应用等多种衍生形态。以小程序为例，作为一种轻量化应用衍生形式，小程序凭借开发便捷、使用灵活等特性，广泛应用于多个行业领域，但也面临潜在安全隐患。一方面，与独立运行的 APP 不同，小程序必须“依附”小程序平台的运行环境获得服务，如通过小程序平台间接获取相应系统权限。在这种模式下，移动应用分发平台无法对小程序进行上架审核，终端也无法实时监测小程序的运行状态，使违法违规小程序有概率绕过现有安全检测监测机制正常运行。另一方面，小程序主要基于云端开发，服务内容可实时更新，开发者仅需简单操作即可实现单个小程序的多平台上线，极大地增加了问题审核和追溯的难度。

类似地，Hybrid App、Web 应用等基于云端内容提供服务的 APP 衍生形态均存在责任链条复杂、难以审核追溯的问题。如何规范新形态 APP 的行为，夯实相关主体的责任，仍然是当前治理工作的难点。

（二）技术应用成为双刃剑，恶意利用亟需防范

技术更新迭代在推动社会数字化转型、提升生产效率的同时，其潜在的恶意利用风险也持续升级。以目前 APP 开发过程中普遍使用的热更新框架为例，热更新技术是指通过动态加载方式将代码或资源装入运行中的 APP，实现 APP 的功能内容即时更新，常用于实现代码热修复、数据统计、内容推送等业务功能，可以有效提高开

发效率。与此同时，热更新技术也容易被恶意开发者利用，成为侵害用户权益、规避合规监管、对抗技术检测的手段。

在移动应用分发平台上架审核和在架投放阶段，部分开发者可将恶意 APP 伪装成正常 APP，当用户下载安装完成后或使用过程中满足某些特定触发条件时，通过热更新的方式下载安装包含恶意代码或违规内容的新版本，实现 APP 的“换装”“变脸”。如某 APP 在用户下载完成后，通过热更新技术将 APP 图标隐藏，使用户无法正常卸载。此外，某些恶意 APP 利用热更新技术，在提供正常服务的同时利用后台静默加载恶意脚本，通过越权、漏洞利用等方式进行安全攻击，危害用户财产和隐私安全。热更新行为触发条件复杂多样，对于现有“人工审查+自动检测”模式而言，增加了恶意 APP 检出难度，降低了检测效率。

（三）AIGC 技术应用广泛，监管治理挑战加剧

AIGC 技术正全方位重塑移动互联网应用的开发逻辑和服务模式，AIGC 模型训练数据规模庞大、来源多样，在模型应用实践中如何准确识别个人信息主体并逐一获得个人信息主体同意缺乏可操作性，知情同意原则难以落地。此外，在模型学习用户偏好、持续迭代优化的过程中，数据使用行为容易超出用户的授权范围。

AI 具备以极低成本完成“以假乱真”的能力，给内容审核、功能性检测带来极大挑战。一方面，AI 工具使用门槛低，增加了 AIGC 技术滥用风险。不法分子可批量炮制伪造新闻，生成误导性信息冲击舆论场；利用 AI 实时换脸，低成本制作以特定人物为主角的视频

或合成通话实施敲诈勒索。另一方面，通过 AI 工具可以快速地批量生产恶意应用，动态改变恶意特征，增大了检测难度。如，AI 可自动重构代码逻辑、修改接口命名或添加冗余代码，生成功能相同的应用变体，极大增加安全检测的样本分析压力。此外，围绕 AI 模型幻觉、AI 价值观对齐、AI 生成内容版权归属的争议也层出不穷。

三、加强分类分级管理，促进行业共识共治

（一）APP 风险分类分级，协作治理正当其时

APP 风险分类分级有助于开发者提升风险意识。通过 APP 风险分类分级，开发者能够清晰认识到不同风险等级的 APP 可能带来的危害，从而在开发过程中更加注重安全设计和隐私保护，有针对性地规范开发运营过程，提高产品安全性。此外，分类分级还能引导开发者进行自查评估，及时发现并修复潜在的安全漏洞，提升 APP 的整体安全水平。

APP 风险分类分级有助于引导用户审慎选择和使用 APP。用户在面对海量 APP 时，往往难以判断其安全性。通过风险分类分级提示，可以帮助用户直观地了解 APP 的风险等级，从而更加安全地选择和使用 APP，避免下载和使用高风险的 APP，保护个人信息和财产安全。

APP 风险分类分级有助于促进生态协作和行业共治。行业共识的 APP 风险分类分级机制可以有效提升治理效率，促进风险信息在产业链上下游的流转和识别，为分发平台对 APP 上架审核及在架监测、智能终端对 APP 的全生命周期管理等产业上下游风险共治提供

参考。

（二）明确分类分级原则，促进准确识别风险

APP 风险分类分级遵循法律法规要求，符合行业现状，并促进风险治理，具体包括以下原则：

合法合规：APP 风险分类分级遵循相关法律法规要求（主要相关法律法规参见附录 A），参考行业实践现状，对监管部门明确下发的风险进行强化分类识别和分级管理。

科学实用：充分考虑不同风险特征，合理设定风险类别，确保覆盖业务实践中的全部风险项，符合业界实际。

公开透明：以简单易懂的语言描述 APP 风险分类分级的标准，公开告知相关开发者、安全厂商等。

动态调整：定期审核和调整 APP 风险分类分级结果，充分考虑行业治理态势和发展趋势，适应 APP 风险治理的政策标准、业务场景等的发展变化。

（三）紧密贴合实际场景，划分具体风险类目

依据风险行为特征不同，结合当前阶段风险 APP 治理的重点，本报告将 APP 风险分为 6 个一级类目，每个一级类目均包含若干二级类目[4](二级风险类目中常见场景详见附 录 B)。

表 1 风险类目

一级风险类目	二级风险类目
隐私安全风险	违规收集个人信息风险
	违规使用个人信息风险

[4] 同一 APP 可能同时存在多种风险

	强制使用定向推送功能风险
	强制频繁过度使用权限风险
恶意行为风险	流氓行为风险
	系统破坏风险
	恶意对抗风险
	热更新篡改风险
	勒索行为风险
	远程控制风险
	恶意传播风险
	漏洞利用风险
	自启动和关联启动风险
	欺骗误导强迫行为风险
	账号注销设置障碍风险
	安装卸载异常行为风险
服务异常风险	运营资质缺失风险
	备案资质缺失风险
	服务功能异常风险
	客诉响应缺失风险
	专有权利侵权风险
	主体经营异常风险
财产安全风险	诱导扣费风险
	自动续费风险
	电信诈骗风险
	诱骗欺诈风险
	诱导投资风险
	金融违规风险
	非法传销风险
	虚假网赚风险
	网络赌博风险

内容安全风险	传播违法信息风险
	传播不良信息风险
未成年人安全风险	内容危害风险
	网络沉迷风险
	隐私侵犯风险

来源：公开资料整理

1.隐私安全风险

（1.1）违规收集个人信息风险

APP 收集个人信息时未征得用户同意、超范围收集或采用恶意攻击手段窃取用户个人信息。

（1.2）违规使用个人信息风险

APP 未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息。

（1.3）强制使用定向推送功能风险

APP 未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项。

（1.4）强制频繁过度使用权限风险

APP 安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭；短时长、高频次，在用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限；未及时明确告知用户索取权限的目的和用

途，提前申请超出其业务功能等权限；对用户正常授予权限预期之外的恶意使用。

2.恶意行为风险

（2.1）流氓行为风险

APP 中存在系统、用户个人信息、资费没有直接损害的其他恶意行为。包括在用户不知情或未授权的情况下，长期占用系统资源、自动捆绑安装、自动修改系统配置，频繁发送骚扰信息，对用户造成打扰等。

（2.2）系统破坏风险

APP 通过感染、劫持、篡改、删除、终止进程等手段导致移动终端或其他非恶意软件部分或全部功能、用户文件等无法正常使用的，干扰、破坏、阻断移动通信网络、网络服务或其他合法业务正常运行的，具有系统破坏属性。

（2.3）恶意对抗风险

APP 通过采取各种技术手段与安全系统进行对抗的行为达到逃避检测和分析的目的。这些技术手段旨在使恶意软件更难被发现、分析和移除。

（2.4）热更新篡改风险

APP 通过热更新恶意代码或云控+热更新的方式控制恶意行为概率性发生，或在特定范围特定条件下发生。

（2.5）勒索行为风险

APP 具有协助或主动攻击、窃取、伪造、破坏系统或用户数据

以勒索用户行为。

（2.6）远程控制风险

APP 能够在用户不知情或未授权的情况下，接受远程控制端指令并进行相关恶意行为操作，具有远程控制属性。

（2.7）恶意传播风险

APP 自动通过复制、感染、投递、下载等方式将自身、自身的衍生物或其他恶意代码进行扩散的行为，具有恶意传播属性。

（2.8）漏洞利用风险

APP 利用已知漏洞（如被 CVE、CNVD、CNNVD 收录）或者未知漏洞（0day）对操作系统或其他 APP 进行攻击，实现权限提升、命令执行、信息窃取、永久拒绝服务等目的，造成安全危害或谋取商业利益的。

（2.9）自启动和关联启动风险

APP 未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方 APP。

（2.10）欺骗误导强迫行为风险

APP 中存在信息窗口关不掉或利用信息窗口页面提供虚假信息、虚假广告，欺骗误导强迫下载、安装、使用第三方 APP 或欺骗误导强迫用户点击跳转第三方页面。

（2.11）账号注销设置障碍风险

APP 中存在账号管理功能，未提供简单便捷的注销方式，或设置不合理障碍阻止用户正常注销。

（2.12）安装卸载异常行为风险

APP 安装后未经用户同意出现多个快捷方式、透明图标，无法卸载或需借助第三方软件才可完成等安装卸载异常问题。

3.服务异常风险

（3.1）运营资质缺失风险

APP 经营范围包含需有关部门前置审批的业务，但未取得相关审批或因审批过期等未达到该行业的许可条件或法律法规要求。

（3.2）备案资质缺失风险

APP 的开发者未按照国家相关法律法规的要求，向相关部门申请完成备案手续。

（3.3）服务功能异常风险

APP 在下载、安装、使用以及卸载过程中所显现的与终端设备适配异常的风险，主要表现为核心功能无法正常使用、功能崩溃等影响用户使用的情况。

（3.4）客诉响应缺失风险

APP 未提供有效的客诉反馈渠道，或不积极响应等行为，严重影响用户体验。

（3.5）专有权利侵权风险

APP 开发者非相关权利所有人且未经相关所有权持有人授权，在 APP 内使用或传播侵犯他人权益的内容，如知识产权（专利权、商标权、著作权等）、肖像权和法律规定的其他权益。

（3.6）主体经营异常风险

APP 资源准入或上线后常规运营阶段，其主体存在经营异常或被注销等情况，可能无法提供正常服务。

4.财产安全风险

（4.1）诱导扣费风险

APP 在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，导致用户被扣费或产生错误认识支付费用。

（4.2）自动续费风险

APP 未征得用户同意或在服务续期前未及时提醒，私自开通自动续订、续费等服务，或在服务期间未提供便捷的取消途径。

（4.3）电信诈骗风险

APP 中存在管理部门认定的涉诈资源或行为。

（4.4）诱骗欺诈风险

APP 采用虚构事实或隐瞒真相等方法诱骗、欺诈用户财产的行为。

（4.5）诱导投资风险

APP 中存在通过夸张夸大等方式诱导用户进行投资等金融活动，实际并未能达到所承诺的投资收益回报，或未依法做风险提示。

（4.6）金融违规风险

金融 APP 开发者从事非法集资、非法虚拟币交易、洗钱等金融交易活动，或未经相关监管部门批准，从事吸收存款、发放贷款、融资担保类金融交易活动。

（4.7）非法传销风险

APP 开发者以推销商品、提供服务等经营活动为名，要求参加者以缴纳费用或者购买商品、服务等方式获得加入资格，并按照一定顺序组成层级，直接或者间接以发展人员的数量作为计酬或者返利依据，引诱、胁迫参加者继续发展他人参加，骗取财物，扰乱经济社会秩序。

（4.8）虚假网赚风险

APP 中存在以网络兼职、刷单、返现等名义诱导用户做任务，但未按约定支付足额酬劳或按期支付酬劳的情况。

（4.9）网络赌博风险

APP 中存在推广非法博彩、宣扬赌博信息，或其他被国家监管部门认定为涉赌的行为和内容。

5.内容安全风险

（5.1）传播违法信息风险

APP 开发者恶意进行内容生产，在 APP 内制作、复制、发布违反我国法律、行政法规以及其他规章规定的内容，或未履行、未压实平台主体责任导致 APP 中存在用户制作、复制、发布相关有害内容且开发者未及时停止传播或采取消除等有效处置。

（5.2）传播不良信息风险

APP 开发者在 APP 内发布、传播对营造清朗的网络空间具有负面作用、扰乱网络秩序、破坏网络生态，导致网络空间戾气横行的不良信息，或未履行、未压实平台主体责任导致 APP 内存在用户制作、复制、发布相关有害内容且开发者未停止传播或采取消除等有

效处置。

6.未成年人安全风险

（6.1）内容危害风险

APP 为未成年人提供网络服务或在未成年人模式下，出现损害未成年人身心健康的内容。

（6.2）网络沉迷风险

APP 开发者未能有效实施时间管理、权限管理、消费管理等措施，导致未成年人沉迷游戏或未经家长同意进行充值。

（6.3）隐私侵犯风险

APP 开发者处理个人信息时能够识别个人信息主体属于未成年人的，但未采取相关措施保护未成年人个人信息与隐私安全。

（四）分级依照风险程度，充分考虑产业影响

1.风险分级方法

对 APP 风险级别的判定，主要考虑该风险影响的对象和该风险对影响对象的损害程度。风险对影响对象造成的损害程度越严重，则风险级别越高。下面分别介绍风险影响对象、风险损害程度、风险级别和他们之间的关系，并给出适用于移动应用分发平台和移动智能终端的 APP 风险定级参考。

2.风险影响对象

APP 关乎社会生活的方方面面，其直接或间接影响对象包括国家安全、社会公序良俗及公共利益、系统安全、公民、法人和其他

组织的合法权益、用户合法权益等。

其中，在系统安全方面，存在影响系统的安全环境和硬件设施、影响终端系统的正常运行、影响终端系统资源正常使用等隐患。

在公民、法人和其他组织的合法权益方面，存在影响法律确认并受法律保护的公民[5]、法人所享有的一定的社会权利和利益的隐患。

在用户合法权益方面，存在影响法律确认的并受法律保护的公民所享有权益的隐患，包括影响用户个人信息权益，用户正常获取服务不被阻断的权利等。

3.风险损害程度

APP 风险对国家安全、社会公序良俗及公共利益、系统安全、公民、法人及其他组织的合法权益、用户合法权益可能造成的损害程度分为三级：一般损害、严重损害、特别严重损害。根据影响对象的不同，同一级别的损害程度分别具有不同的表现形式。下面给出划分损害程度的判断原则。

表 2 APP 风险损害程度[6]

影响对象	程度判断原则	损害程度
国家安全	导致国家安全受到影响	特别严重损害
社会公序良俗及公共利益	波及部分地区、少量群体，对社会公序良俗及公共利益造成一般影响。	一般损害
	波及多个地区、一定量的群体，对社会公序良俗及公共利益造成严重影响。	严重损害
	波及大量地区和群体，对社会公序良俗及公共利益造	特别严重损

[5] 此处公民指相对于 APP 使用者以外的其他合法公民

[6] 损害程度主要参考 GB/T 20986-2023、GB/T 22240-2020、GB/T 43697-2024、YD/T 6008-2024 等标准

	成特别严重影响。	害
系统安全	长期不合理占用系统资源，用户无感知且未造成用户实际财产损失。	一般损害
	导致用户无法正常使用。如 APP 主体存在协助或主动攻击、破坏、控制等行为，造成用户无法正常使用系统或软件服务的。	严重损害
	导致用户造成财产损失。如 APP 主体存在协助、伪造用户操作等行为，造成用户财产损失的。	特别严重损害
公民、法人和其他组织的合法权益	波及少量群体，对公民、法人的财产、声誉、正常生产生活等造成一般影响。	一般损害
	波及一定量群体，对公民、法人的财产、声誉、正常生产生活等造成严重影响。	严重损害
	波及大量群体，对公民、法人的财产、声誉、正常生产生活等造成特别严重影响。	特别严重损害
用户合法权益	波及少量群体，对用户个人信息权益、正常获取服务的权益等造成一般影响。	一般损害
	波及一定量群体，对用户个人信息权益、正常获取服务的权益等造成严重影响。	严重损害
	波及大量群体，对用户个人信息权益、正常获取服务的权益等造成特别严重影响。	特别严重损害

来源：公开资料整理

4.风险级别划分

根据 APP 风险对不同影响对象的不同损害程度，将 APP 风险级别分为四级：极高、高、中、低，以下给出单个 APP 风险的级别划分规则。需要注意的是，对风险 APP 进行分级时，应遵循就高原则，即如某 APP 同时具有多重风险，应将风险级别划分为其中的最高级别。

表 3 APP 风险级别划分

影响对象	损害程度		
	一般损害	严重损害	特别严重损害
国家安全	极高		
社会公序良俗及公共利益	低	中	高/极高
终端系统安全	低	中	高/极高
法人、其他组织的合法权益	低	中	高/极高
用户合法权益	低	中	高/极高

来源：公开资料整理

5.风险分级参考

参考前文所述风险损害程度、风险等级划分，并结合恶意行为主动程度、APP 违规频次、治理优先级等多重因素综合考量，不同情况可对应不同风险等级。

表 4 风险分级参考

风险类别序号	风险类别	风险级别范围
1.1	违规收集个人信息风险	低级到高级
1.2	违规使用个人信息风险	低级到高级
1.3	强制使用定向推送功能风险	低级到中级
1.4	强制频繁过度使用权限风险	低级到高级
2.1	流氓行为风险	低级到高级
2.2	系统破坏风险	中级到极高
2.3	恶意对抗风险	中级到极高
2.4	热更新篡改风险	中级到极高
2.5	勒索行为风险	中级到极高

2.6	远程控制风险	中级到极高
2.7	恶意传播风险	中级到极高
2.8	漏洞利用风险	中级到极高
2.9	自启动和关联启动风险	低级到中级
2.10	欺骗误导强迫行为风险	低级到高级
2.11	账号注销设置障碍风险	低级到中级
2.12	安装卸载异常行为风险	低级到中级
3.1	运营资质缺失风险	低级到高级
3.2	备案资质缺失风险	低级到高级
3.3	服务功能异常风险	低级到中级
3.4	客诉响应缺失风险	低级到中级
3.5	专有权利侵权风险	低级到高级
3.6	主体经营异常风险	低级到中级
4.1	诱导扣费风险	低级到高级
4.2	自动续费风险	低级到高级
4.3	电信诈骗风险	极高
4.4	诱骗欺诈风险	低级到极高
4.5	诱导投资风险	低级到极高
4.6	金融违规风险	低级到极高
4.7	非法传销风险	中级到极高
4.8	虚假网赚风险	低级到高级
4.9	网络赌博风险	中级到极高
5.1	传播违法信息风险	低级到极高
5.2	传播不良信息风险	低级到高级
6.1	内容危害风险	低级到极高
6.2	网络沉迷风险	低级到高级
6.3	隐私侵犯风险	低级到极高

来源：公开资料整理

对于“低、中、高、极高”不同风险等级，在 APP 全生命周期的各个阶段，APP 开发者、移动应用分发平台、移动智能终端等主体可采取不同程度的管理措施。在 APP **开发**阶段，APP 企业内部参照风险分类分级进行自查自纠，辅助合规开发。对接入的第三方 SDK，第三方页面等进行供应链安全风险审核。APP 企业同步建立全流程合规的内控机制，根据在开发、测试、更新、第三方接入等环节发现的风险问题，综合评估应对措施。在 APP **上架审核**阶段，重点审查 APP 安全性和合规性，采取“风险提示”（明确风险信息供用户下载参考）、“限制分发”或“不予上架”等形式的管控措施。在 APP **在架监测**阶段，建立健全在架巡检机制，采取“通知开发者限期整改”“下架应用”“冻结应用”“冻结开发者”等形式的管控措施，并根据开发者的违规记录建立信用评价机制，综合评估 APP 风险等级。在 APP **下载安装**阶段，加强安装环节的风险检测能力，采取“风险提示”“用户授权确认”“禁止安装”等形式的管控措施。在 APP **运行**阶段，实时监测 APP 的运行状态、用户反馈等信息，及时发现异常情况和潜在风险，采取“风险提示”“引导用户卸载”“启动预警”“启动拦截”等形式的管控措施，并建立 APP 恶意行为风险监测机制，根据 APP 的风险行为综合评估 APP 风险等级。

附 录 A 相关法规

（一）法律

《中华人民共和国个人信息保护法》（2021.11.1 实施）

《中华人民共和国数据安全法》（2021.9.1 实施）

《中华人民共和国网络安全法》（2017.6.1 实施）

《中华人民共和国反电信网络诈骗法》（2022.12.1 实施）

《中华人民共和国未成年人保护法》（2024.4.26 修正）

《中华人民共和国消费者权益保护法》（2013.10.25 修正）

《中华人民共和国广告法》（2021.4.29 实施）

（二）行政法规

《网络数据安全管理条例》（2025.1.1 实施）

《中华人民共和国电信条例》（2016.2.6 修订）

《中华人民共和国计算机信息系统安全保护条例》（2011.1.8 修订）

《未成年人网络保护条例》（2024.1.1 实施）

《中华人民共和国消费者权益保护法实施条例》（2024.7.1 实施）

《信息网络传播权保护条例》（2013.3.1 实施）

《禁止传销条例》（2005.11.1 实施）

《防范和处置非法集资条例》（2021.5.1 实施）

（三）部门规章

《电信和互联网用户个人信息保护规定》（2013.9.1 实施）

《数据出境安全评估办法》（2022.9.1 实施）

《通信网络安全防护管理办法》（2010.3.1 实施）

《网络安全审查办法》（2022.2.15 实施）

《儿童个人信息网络保护规定》（2019.10.01 实施）

《互联网信息服务算法推荐管理规定》（2022.3.1 实施）

《互联网信息服务深度合成管理规定》（2023.1.10 实施）

《生成式人工智能服务管理暂行办法》（2023.8.15 实施）

《个人信息保护合规审计管理办法》（2025.5.1 实施）

《互联网广告管理办法》（2023.5.1 实施）

《互联网文化管理暂行规定》（2017.12.15 修订）

《互联网新闻信息服务管理规定》（2017.6.1 实施）

《网络出版服务管理规定》（2016.3.10 实施）

《互联网药品信息服务管理办法》（2017.11.17 实施）

《电信业务经营许可管理办法》（2017.9.1 实施）

《互联网视听节目服务管理规定》（2015.8.28 修订）

（四）规范性文件

《APP 违法违规收集使用个人信息行为认定方法》（2019.12.30 发布）

《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》（2019.10.31 发布）

《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（2020.7.24 发布）

《常见类型移动互联网应用程序必要个人信息范围规定》

（2021.5.1 实施）

《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》（2023.2.6 实施）

《云计算服务安全评估办法》（2019.9.1 实施）

《关于开展网络安全服务认证工作的实施意见》（2023.3.15 实施）

《关于开展 2020“清朗”未成年人暑期网络环境专项整治的通知》（2020.7.9 发布）

《文化和旅游部办公厅关于加强网络文化市场未成年人保护工作的意见》（2021.11.29 发布）

《移动互联网未成年人模式建设指南》（2024.11.15 发布）

《移动互联网应用程序信息服务管理规定》（2022.8.1 实施）

《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》（2018.11.30 实施）

《工业和信息化部关于开展移动互联网应用程序备案工作的通知》（2023.8.4 发布）

《互联网弹窗信息推送服务管理规定》（2022.9.30 实施）

《广告绝对化用语执法指南》（2023.2.25 发布）

《互联网广告可识别性执法指南》（2024.8.22 发布）

《网络音视频信息服务管理规定》（2020.01.01 实施）

《关于整治虚拟货币“挖矿”活动的通知》（2021.9.3 发布）

《关于进一步防范和处置虚拟货币交易炒作风险的通知》

（2021.9.15 发布）

附 录 B APP 风险场景

本报告依据风险行为特征，结合当前风险 APP 治理重点，在 APP 风险分类的 6 个一级类目和细分的二级类目基础上，进一步对二级类目风险的常见风险场景进行梳理，便于行业上下游参考使用。

1.隐私安全风险

（1.1）违规收集个人信息风险

包括但不限于以下场景:

a）APP 收集个人信息前未向用户明示或未清晰明示个人信息处理的目的、方式和范围;

b）APP 未向用户明示或未清晰明示第三方 SDK 处理个人信息的目的、方式和范围;

c）APP 或其所集成的第三方 SDK 在用户不知情或未授权情况下收集个人信息;

d）APP 在收集个人信息征求用户同意时，未提供明确的同意和拒绝选项，或设置为默认同意;

e）APP 广告页面、开屏广告、主屏等功能页面，以积分、奖励、优惠等方式欺骗误导用户提供身份证号、人脸、指纹等个人信息;

f）APP 或其所集成的第三方 SDK 在收集个人信息时，超出其所明示收集目的的合理关联范围;

g）APP 或其所集成的第三方 SDK 在收集个人信息时，以特定

频率收集个人信息或收集频率超出其实现产品或服务的业务功能所必需的最低频率;

h）APP 在用户不知情或未授权的情况下，通过恶意代码植入、系统运行监控、网络信息嗅探等方式获取用户个人信息，具有恶意隐私窃取属性;

i）APP 在收集生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息时，未征得用户的单独同意。

（1.2）违规使用个人信息风险

包括但不限于以下场景:

a）APP 未向用户明示个人信息处理的目的、方式和范围，将个人信息发送给第三方 SDK 等产品或服务;

b）APP 以个人信息处理规则弹窗等形式向用户明示共享给第三方的行为，未经用户同意，将个人信息发送给第三方 SDK 等产品或服务;

c）APP 以个人信息处理规则弹窗等形式向用户明示个人信息处理的目的、方式和范围，未清晰明示共享的第三方身份、目的及个人信息类型，用户同意后，将个人信息发送给第三方 SDK 等产品或服务;

d）APP 未向用户告知且未经用户同意，将设备识别信息、商品浏览记录、搜索使用习惯、软件安装列表等个人信息传输至 APP 服务器后，向第三方产品或服务提供其收集的个人信息。

（1.3）强制使用定向推送功能风险

包括但不限于以下场景:

a）若 APP 的业务功能存在定向推送功能，未以个人信息处理规则弹窗等形式向用户明示，将收集的用户个人信息用于定向推送、精准营销;

b）若 APP 定向推送功能使用了第三方的个人信息来源，未以个人信息处理规则弹窗等形式向用户明示业务功能使用第三方的个人信息进行定向推送，且未向用户明示第三方的个人信息来源;

c）APP 以个人信息处理规则弹窗等形式明示存在定向推送功能，页面中未通过标明“个性化推荐”“定推”“猜你喜欢”等其他能区分个性化内容的字样，或通过不同的栏目、版块、页面分别展示等显著方式区分定向推送服务;

d）APP 以个人信息处理规则弹窗等形式明示存在定向推送功能，未提供便捷有效的退出或关闭个性化展示模式的选项，如拒绝接受定向推送信息，或停止、退出、关闭相应功能的机制。

（1.4）强制频繁过度使用权限风险

包括但不限于以下场景:

a）APP 运行时，向用户索取权限，用户拒绝授权后，APP 退出或关闭，拒绝注册或登录，或拒绝提供与申请权限无关的功能服务;

b）APP 运行时，向用户索取权限，用户拒绝授权后，APP 循环弹窗申请权限，使用户无法继续使用;

c）APP 未提供相关业务功能或服务，申请权限;

d）APP 首次打开或运行中，未见使用权限对应的相关功能或服

务时，提前向用户弹窗申请开启权限;

e）APP 频繁申请权限，具体场景包括但不限于以下方式：APP 运行时，在用户明确拒绝权限申请后，向用户频繁弹窗申请与当前服务场景无关的权限，影响用户正常使用。APP 在用户明确拒绝权限申请后，重新运行时，APP 向用户频繁弹窗申请开启与当前服务场景无关的权限，影响用户正常使用;

f)APP 向用户索取权限时，未同步告知用户申请该权限的目的;

g）APP 滥用敏感权限、特殊权限等实现非正常业务功能。

2.恶意行为风险

（2.1）流氓行为风险

包括但不限于以下场景:

a）在用户不知情或未授权的情况下，长期驻留系统内存;

b）在用户不知情或未授权的情况下，长期占用移动终端中央处理器计算资源;

c）在用户不知情或未授权的情况下，自动捆绑安装;

d）在用户不知情或未授权的情况下，自动添加、修改、删除收藏夹、快捷方式;

e）在用户不知情或未授权的情况下，修改系统配置信息;

f）导致用户无法正常退出;

g）伪装成系统按键;

h）在用户不知情或用户未授权的情况下，执行其他操作的，如频繁连接网络、自动发送短信或彩信等;

i）频繁发送骚扰信息，如短信、通知栏、站内信等，对用户造成打扰。

（2.2）系统破坏风险

包括但不限于以下场景:

a）导致移动终端硬件、操作系统、其他软件无法正常工作;

b）导致移动终端网络通讯功能无法正常使用;

c）导致移动终端电池电量非正常消耗;

d）导致移动终端基本功能无法正常工作;

e）导致移动终端基本性能出现异常;

f）导致其他合法业务无法正常运行;

g）对用户文件、系统文件或其他软件进行感染、劫持、篡改的;

h）在用户不知情或未授权的情况下，对系统文件或其他软件进行删除、卸载、终止进程或限制运行;

i）在用户不知情或未授权的情况下，对用户文件进行删除。

（2.3）恶意对抗风险

包括但不限于以下场景:

a）通过控制网页跳转隐藏或者控制恶意功能，不良内容等的展示;

b）提供游戏外挂功能，破坏游戏公平性，窃取用户账号数据，窃取用户虚拟资产等;

c）通过模拟用户操作、APP 多开分身等方式进行广告欺诈、账号刷单等;

d）提供破解其他 APP 或绕过其他 APP 安全机制的功能。

（2.4）热更新篡改风险

包括但不限于以下场景:

a）开发者在应用商店上架时，上架的包为正常应用，通过上架审核后，用户下载安装后热更新成另外一个未经审核的应用;

b）开发者对同一个应用克隆出多个马甲包，通过上架审核后，用户下载安装后，热更新动态修改马甲包，引导用户/自动更新变为另外一个应用;

c）用户安装 APP 后，正常功能保持不变，在后台热更新加载新的插件，根据操作系统版本，不断尝试漏洞提取，破坏系统，危害用户财产和隐私安全;

d）APP 上架后，未经用户同意通过热更新在用户无感的情况下变更隐私数据采集行为，和隐私政策中告知用户同意的内容不相符;

e）APP 一方面热更新绕过平台技术检测，一方面通过云控的方式控制恶意行为概率发生，或者在特定范围内、特定条件下发生，造成技术对抗，恶意提高监管和监测的难度和成本。

（2.5）勒索行为风险

包括但不限于以下场景:

a）导致移动智能终端锁屏、输入输出异常等使软硬件无法正常工作，并存在勒索提示信息;

b）导致移动智能终端内或应用内的文本、文档、图片、用户数据等被加密、篡改、窃取或破坏，并存在勒索提示信息;

c）通过 APP 非法获取用户隐私数据，经用户举报存在勒索行为；

d）APP 具有其他协助或主动攻击、窃取、伪造、破坏系统或用户数据以勒索用户行为。

（2.6）远程控制风险

包括但不限于以下场景：

a）由控制端主动发出指令进行远程控制；

b）由受控端主动向控制端请求指令。

（2.7）恶意传播风险

包括但不限于以下场景：

a）自动发送包含恶意代码或恶意代码链接的短信、彩信、邮件、WAP 信息等；

b）自动利用蓝牙、红外、无线网络等技术向其他设备发送恶意代码；

c）自动向存储卡等移动存储设备上复制恶意代码；

d）自动下载恶意代码；

e）自动感染其他文件；

f）通过欺骗性手段或者提供误导性信息，诱导用户下载安装其他风险应用。

（2.8）漏洞利用风险

包括但不限于以下场景：

a) 利用漏洞打开其他 App 的保护组件，绕过安卓沙箱的限制；

b) 利用漏洞获取系统敏感权限，或者干扰用户正常使用。

（2.9）自启动和关联启动风险

包括但不限于以下场景:

a）未向用户明示未经用户同意，且无合理的使用场景，自启动或关联启动其他 APP;

b）向用户明示但未经用户同意，自启动或关联启动其他 APP;

c）非服务所必需或无合理应用场景，自启动或关联启动第三方 APP;

d)SDK 非服务所必需或无合理应用场景,启动或关联启动 APP。

（2.10）欺骗误导强迫行为风险

包括但不限于以下场景:

a）用户通过 APP 信息窗口页面下载的 APP 与信息窗口向用户所做的宣传或者承诺不符;

b）在用户无操作情况下 APP 信息窗口页面自动下载、安装、使用第三方 APP;

c）APP 信息窗口页面，无显著第三方 APP 下载提示，用户点击广告或其他页面区域即自动下载;

d）用户暂停或取消 APP 内下载、安装第三方 APP 自动恢复下载安装行为;

e）APP 信息窗口页面，通过虚假、引人误解的方式欺骗误导强迫用户下载、安装第三方 APP，包括但不限于在未明示下载第三方 APP 的具体情况下，通过“立即登录”“开始游戏”“领取红包”“手机卡

顿”“开具发票”等方式；

f）在用户点击下载后，APP 分发页面未同步展示下载进度并提供暂停、取消选项，或未以显著方式告知查看下载进度及提供暂停、取消选项；

g）非服务所必需或无合理场景，以弹窗等方式强迫用户更新 APP；

h）APP 抄袭其他 APP 名称、图标、简介等具有可识别特性的特征信息山寨仿冒以达到欺骗误导用户下载使用的目；

i）APP 以欺骗、误导或者强迫等方式向用户提供互联网信息服务或者产品；

j）APP 信息窗口页面，存在欺骗误导强迫用户跳转的文字、图片或视频链接；

k）APP 中存在频繁弹窗干扰用户正常使用的行为；

l）APP 停止使用后仍在应用外的其他界面弹出广告；

m）APP 广告未明示“广告”标识，未与其他非广告信息相区别，误导用户点击；

n）APP 未以显著方式明示或未经用户主动选择同意，其信息窗口页面，存在跳转、使用第三方 APP 的行为；

o）APP 信息窗口通过用户“摇一摇”等交互动作触发页面或第三方 APP 跳转的，未清晰明示用户需要执行的触发动作及交互预期，或通过设置高灵敏度降低交互动作判定阈值，造成误导、强迫式跳转。

（2.11）账号注销设置障碍风险

包括但不限于以下场景:

a）APP 未向用户提供注销账户的方法，且方法不简便，难操作;

b）注销服务设置不合理的障碍，如注销时候身份验证提供的信息多于注册、使用等服务环节收集的个人信息、要求个人信息主体填写精确的历史操作记录、注册满一定周期才能注销等。

（2.12）安装卸载异常行为风险

包括但不限于以下场景:

a）未征得用户同意，APP 安装后出现多个桌面快捷方式、透明图标或无图标;

b）APP 无法卸载或需借助第三方软件才可卸载。

3.服务异常风险

（3.1）运营资质缺失风险

包括但不限于以下场景:

a）APP 开发者未按照法律、行政法规以及国家有关规定具备 APP 经营范围对应的资质证明;

b）APP 开发者具备的资质证明未在有效期内或与经营范围不符等情形;

c）APP 开发者篡改，伪造相关资质或冒用、盗用他人资质文件。

（3.2）备案资质缺失风险

包括但不限于以下场景:

a）APP 未按照电信主管部门要求进行 APP 备案;

b）APP 涉及面向境内公众提供具有舆论属性或者社会动员能力的生成式人工智能服务的，未履行备案程序；

c）游戏类 APP 未履行出版备案程序；

d）金融类 APP 未履行移动金融 APP 备案程序；

e）APP 未履行其他法定备案程序。

（3.3）服务功能异常风险

包括但不限于以下场景：

a）APP 无法正常安装、启动，包括但不限于下载失败、无法安装、无法退出、严重卡顿、闪退、黑屏、无响应等各类功能异常情况，或需借助第三方软件才可安装的情况；

b）APP 不得在注册或登录过程中出现异常，包括但不限于无法接收短信验证码、账号不可用等异常情况；

c）APP 已停止运营服务，存量用户无法正常使用应用内已充值/续费的功能。

（3.4）客诉响应缺失风险

包括但不限于以下场景：

a）APP 中未提供有效的客诉反馈渠道、举报受理机制及入口；

b）APP 对用户投诉问题未在规定时间内进行处理。

（3.5）专有权利侵权风险

包括但不限于以下场景：

a）APP 开发者不享有软件著作权且未经授权使用他人软件上架；

b）APP 开发者使用商标、品牌标识等他人具有知识产权的内容，

不具备商标证明或第三方授权;

c）APP 开发者使用他人专利，不具备专利证明或授权;

d）APP 开发者使用真实人物形象，不具备相关授权。

（3.6）主体经营异常风险

包括但不限于以下场景:

a）APP 主体公司在《国家企业信用信息公示系统》内显示经营状态为“异常”;

b）APP 主体公司工商登记经营状态为“吊销”“注销”等异常状态。

4.财产安全风险

（4.1）诱导扣费风险

包括但不限于以下场景:

a）APP 在用户不知情或未授权的情况下为用户自动订购移动增值业务或其他付费业务;

b）APP 在用户不知情或未授权的情况下自动利用移动终端支付功能进行消费;

c）APP 内未遵守明码标价等相关规定，真实准确、醒目规范地明示收费标准、收费方式等信息，扣除用户会员费，手续费等服务资费;

d）APP 扣费前未经用户确认进行恶意扣费行为，如：未在商品购买和商品支付界面提供给用户进行二次确认;

e）APP 的付费使用条件与明示的信息不一致，在付费后仍存在其他未明示的限制条件，并以此为由终止用户正常使用的产品功能

和服务;

f）APP 公示资费内容时存在明显缩小字体大小、弱化字体颜色（相较于相关说明板块的常规文字要素）等方式隐瞒主要信息，误导用户付费。

（4.2）自动续费风险

包括但不限于以下场景:

a）APP 未征得用户同意，以默认勾选、强制捆绑等方式开通自动续订、自动续费方式的服务;

b）APP 在自动续订、自动续费服务期间未提供便捷的随时退订方式和自动续订、自动续费取消途径;

c）APP 在自动续订、自动续费前未提前 5 日以短信或浮窗通知栏消息推送等显著方式及时提醒用户。

（4.3）电信诈骗风险

包括但不限于以下场景:

a)APP 包体文件中包含公安机关认定的涉诈骗 IP、域名或 URL;

b）APP 包体文件中包含已被公安机关标记的涉诈资源，包括但不限于涉诈关键词、涉诈多媒体数据等;

c）APP 明确为管理部门认定的具有涉诈风险的 APP，或经过用户举报标记为涉诈 APP 且经判定后涉诈风险高;

d）APP 开发者被管理部门认定为诈骗组织或人员;

e）下载链接域名为公安机关认定的涉诈网址域名。

（4.4）诱骗欺诈风险

包括但不限于以下场景：

a）APP 中存在通过社交交友、色情诱导等方式诱骗用户付费或充值的情况；

b）APP 中存在通过伪装为系统或其他应用向用户发送通知，欺骗用户执行付费操作的情况；

c）APP 开发者通过后台操纵 APP 中射幸玩法诱骗用户付费投入；

d）APP 中存在假冒或冒充正规官方 APP 诱骗他人财物；

e）APP 中存在虚构交易内容/投资模式，引导用户进行付费或投资；

f）APP 发布虚假兼职、网赚等信息，诱导用户转账或付费；

g）APP 主体注册信息异常，存在使用虚假注册信息或冒用他人信息注册 APP；

h）通过伪造、篡改、劫持短信、彩信、邮件、通信录、通话记录、收藏夹、桌面等方式诱骗用户付费，以达到诈骗目的；

i）利用 AI 技术生成虚假、伪造不实的信息内容，诱导用户产生错误的认知，导致用户财产损失。

（4.5）诱导投资风险

包括但不限于以下场景：

a）APP 提供金融产品或服务但未做合理风险提示；

b）APP 中存在对投资理财类产品的收益回报、未来效果等进行虚假宣传，如明示或者暗示保本、无风险或者保收益。

（4.6）金融违规风险

包括但不限于以下场景：

a）APP 开发者未经相关监管部门批准，无经营许可证从事相关金融交易活动；

b）APP 中存在涉及虚拟货币或虚拟货币衍生品的交易服务；

c）APP 中存在以介绍费、咨询费、管理费、逾期利息、违约金等名义和以从本金中预先扣除等方式收取利息，超过国家金融部门年利率要求的发放高利贷行为；

d）APP 为无贷款资质的产品进行推广引流；

e）APP 开发者直接或间接为犯罪分子提供非法转移资金、转移违法所得的渠道，如直播 APP 提供支付接口给黑灰产平台后通过提现实现“假直播真洗钱”。

（4.7）非法传销风险

包括但不限于以下场景：

APP 中存在通过给予红包、返现等奖励形式鼓励用户发展下线，要求被发展人员以交纳一定费用或者以认购商品等方式变相交纳费用为条件来取得加入资格，同时以发展数量为依据对不同层级设置高低不等的分成奖励。

（4.8）虚假网赚风险

包括但不限于以下场景：

a）APP 在用户提现时设置重重障碍，导致提现困难延期提现；

b）APP 在用户任务达成时，恶意判定用户任务完成失败，导致

用户无法达成提现条件。

（4.9）网络赌博风险

包括但不限于以下场景:

a）APP 隐私政策、用户协议等域名为公安机关认定的涉赌博类网站 IP、域名或 URL;

b）APP 内为用户提供可直接或间接投入法定货币或虚拟货币参与的“抽奖”“一元夺宝”“玩转盘”“猜大小”等射幸玩法，并为用户提供法定货币的反向兑换服务。

5.内容安全风险

（5.1）传播违法信息风险

包括但不限于以下场景:

a）APP 中存在反对宪法所确定的基本原则的内容;

b）APP 中存在危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的内容;

c）APP 中存在损害国家荣誉和利益的内容;

d）APP 中存在歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的内容;

e）APP 中存在宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的内容;

f）APP 中存在煽动民族仇恨、民族歧视，破坏民族团结的内容;

g）APP 中存在破坏国家宗教政策，宣扬邪教和封建迷信的内容;

h）APP 中存在散布谣言，扰乱经济秩序和社会秩序的内容;

i）APP 中存在散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的内容;

j）APP 中存在侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的内容;

k）利用 AI 模型生成，并发布或传播违法信息。

（5.2）传播不良信息风险

包括但不限于以下场景:

a）APP 中存在使用夸张标题，内容与标题严重不符的内容;

b）APP 中存在炒作绯闻、丑闻、劣迹等的内容;

c）APP 中存在不当评述自然灾害、重大事故等灾难的内容;

d)APP 中存在带有性暗示、性挑逗等易使人产生性联想的内容;

e）APP 中存在展现血腥、惊悚、残忍等致人身心不适的内容;

f）APP 中存在煽动人群歧视、地域歧视等的内容;

g）APP 中存在宣扬低俗、庸俗、媚俗内容的内容。

6.未成年人安全风险

（6.1）内容危害风险

包括但不限于以下场景:

a）APP 未在未成年模式下为未成年人提供分龄适龄内容;

b）APP 中存在宣扬淫秽、色情、暴力、邪教、迷信、赌博、引诱自残自杀、恐怖主义、分裂主义、极端主义等危害未成年人身心健康内容的网络信息，尤其是有关未成年人的淫秽色情网络信息;

c）APP 的首页首屏、弹窗、热搜等醒目位置或专门以未成年人为服务对象的产品和服务中存在可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等可能影响未成年人身心健康的信息;

d）APP 向未成年人发送、推送或者诱骗、强迫未成年人接触含有危害或者可能影响未成年人身心健康内容的网络信息;

e）APP 中存在以文字、图片、音视频等形式，对未成年人实施侮辱、诽谤、威胁或者恶意损害形象等网络欺凌行为，或未建立健全网络欺凌行为的预警预防、识别监测和处置机制;

f）APP 中存在以文字、图片、音视频等形式，组织、教唆、胁迫、引诱、欺骗、帮助未成年人实施违法犯罪行为。

（6.2）网络沉迷风险

包括但不限于以下场景:

a）网络游戏、网络直播、网络音视频、网络社交等 APP 开发者未对未成年人使用其服务设置相应的时间管理、权限管理、消费管理等功能;

b）以未成年人为服务对象的在线教育网络产品和服务插入网络游戏链接，或推送广告等与教学无关的信息;

c）向未成年人提供网络游戏账号租售服务的信息，以问答等形式教授破解防沉迷系统;

d）设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，或利用泛娱乐化功能和内容诱导未成年人沉迷网络;

e）游戏 APP 开发者未要求以真实身份信息注册并登录网络游戏的;

f)游戏 APP 开发者未按要求对游戏产品进行分类并作出适龄提示的。

（6.3）隐私侵犯风险

包括但不限于以下场景:

a）APP 开发者处理未成年人个人信息前，未能在个人信息处理规则中设置专门的未成年人个人信息保护的条款;

b）APP 开发者在处理未满十四周岁未成年人个人信息前，未能制定并公开单独成文的儿童个人信息保护规则，未依法征得未成年人父母或者其他监护人的明示同意;

c）APP 开发者处理未成年人个人信息的，未遵循合法、正当和必要的原则;

d)APP 含直播功能但未采取措施对未满十六周岁的未成年人进行直播管控。

中国信息通信研究院 泰尔终端实验室

中国信息通信研究院 技术与标准研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62300498 010-62300568

传真：010-62300586

网址：www.caict.ac.cn