ICS 35.240.99
CCS L70/84

T/

团 体 标 准

T/CCIASC 0049—2025

平台生态安全分级保护基本要求

Basic Requirements for Security Classification Protection of Platform Ecosystems

（征求意见稿）

2025－08－XX 发布 2025－08－XX 实施

中国计算机行业协会 发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》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专利的责任。

本文件由中国计算机行业协会提出。

本文件由中国计算机行业协会归口。

本文件起草单位：蚂蚁科技集团股份有限公司、中国软件评测中心、蚂蚁智安安全技术（上海）有限公司、上海交通大学、安恒信息技术有限公司、北京百度网讯科技有限公司

本文件主要起草人：邵晓东，宋铮，郑亮，张可菁、陈静男、唐佳伟、姜志辉、唐刚、张德馨、安健、杨志、张学扬、谷大武、孙士锋、付婧妍、陈星、何佳、吴月升、裘盼盼、杜人可、石翼、陈嘉茵、甘甜、蒋荣、徐玮、朱强强、冯朝、晋知文、牛雅威、吴映京、鲁袁伟、曾庆瑜、唐艺嘉、曹琳、杨刚、张晓旭、武玥、崔梦、温颖颀

引　言

互联网平台既是企业的重要商业平台，也是网民生活、工作的公共空间，掌握了关系国计民生的大量资源。随着数字经济的不断发展，数字经济业务模式越来越复杂，互联网平台面临越来越复杂的网络安全风险包括用户隐私泄露、网络欺诈、网络安全和信息不准确性等各方面，平台生态安全风险很容易传导影响社会稳定、公共利益。

本标准有助于进一步评估发现可能影响社会稳定、公共利益的网络安全风险，保障生态机构自身做好安全防护，降低自身安全风险的同时更好的帮助平台生态机构，保障生态机构从入驻审核、过程管控、退出保障等全生命周期安全管理尽责，做好安全保护；保障生态机构自身从网络安全、数据安全、内容安全、资金安全等方面的安全能力建设，助力生态机构降低自身安全风险。促进整体平台生态安全水位的提升，帮助平台及生态机构充分发挥数据要素价值，促进数字经济产业发展。

平台生态安全分级保护基本要求

1 范围

本文件给出了平台运营者和平台生态机构的安全管理要求。

本文件适用于指导平台及平台生态机构搭建安全保护能力，履行网络安全、个人信息保护和数据安全等相关责任提供指导，旨在帮助组织更好满足安全合规要求。

。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 45404-2025 数据安全技术 大型互联网企业内设个人信息保护监督机构要求

GB/T 44588-2024 数据安全技术 互联网平台及产品服务个人信息处理规则

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2019 信息安全技术 网络安全等级保护定级指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

TC260-PG-20243A 网络安全标准实践指南—大型互联网平台网络安全评估指南

3 术语和定义

GB/T 38664.1—2020界定的以及下列术语和定义适用于本文件。

3.1

平台 internet platform

即互联网平台，通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。

[来源：TC260-PG-20243A，术语和定义2.1]

3.2

平台运营者 platform operator

向自然人、法人及其他市场主体提供经营场所、交易撮合、信息发布等互联网平台服务的法人及非法人组织。

3.3

平台生态机构 platform ecosystem institution

在互联网平台内提供商品或者服务的经营者。

3.4

数据安全网关 data security gateway

可承载跨主体(包含外部主体)数据流通且具备数据管控能力的系统，一般由运行态和管理态共同构成。运行态指数据跨主体流通时实时的数据流动过程，管理态指数据跨主体流通时事前的管理流程和机制。

3.5

敏感个人信息 sensitive personal information

一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

[来源:GB/T 35273-2020，定义3.2]

4 平台运营者安全基本要求

4.1 安全基本要求

平台应满足对应的网络安全等级保护安全要求，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理、安全运维管理等要求。具体参照GB/T 22239-2019《网络安全等级保护基本要求》。

4.2 组织保障

4.2.1 管理制度

a）平台运营者应建立安全管理制度，包括但不限于网络安全、数据安全、资金安全、内容安全等各关键领域的管理要求。

4.2.2 组织建设

a）平台运营者应建立相关的安全管理组织，明确架构层级、职责划分以及人员的具体分工，建立清晰的岗位职责、奖惩制度、考核机制。

4.2.3 安全能力

a）平台运营者应确保相应的安全管理人员应具备岗位所需的能力。

b）平台运营者应定期对相应的安全管理人员进行相应的培训、考核。

4.3 安全管理

a）平台运营者应对生态机构主体信息进行实名认证核实，生态机构主体信息包含不限于身份信息、联系方式、工商证照等。

b）平台运营者应对生态机构提供的资质证明文档进行形式审核，如提供金融、新闻、出版、医疗保健、药品和医疗器械、社交、游戏等互联网信息服务。

c）平台运营者应制定生态机构准入管理规则、保障用户个人信息权益的用户信息处理规范、横跨数据安全全生命周期管控的生态机构安全管理规范、约束服务商对商户提供运营/推广/开发服务的服务商管理规范、针对特殊应用类型生效的小程序/生活号运营规范、以及定义生态机构违规处置的违规处理规范等。

d）平台运营者应参照相关国家标准，规范生态机构运营行为，保障用户的合法权益和社会公共利益；保证生态机构在为用户提供产品和服务的过程中，严格遵守中华人民共和国相关法律法规的要求；

e）平台运营者应制定安全分级保护要求，生态机构应满足对应等级要求。

f）对未达到对应安全能力要求或未按时完成安全能力评估的生态机构，平台运营者应限制其获取相关权限及服务。

4.4 安全评估

a）平台运营者应对生态伙伴，周期性组织进行安全能力评估工作，确保满足相应安全能力要求后平台放行机构准入或数据开放过程；包括但不限于组织管理与机制、数据安全生命周期管理、系统安全、网络安全、内容安全、资金安全等部分。

b）应对未能满足安全能力要求的生态机构，约束平台相关权限或服务。

c）平台运营者应使用技术检测能力，对生态机构的安全能力情况进行跟踪监测。

d）平台运营者应通过功能验证、技术检测、文档审查等方式对生态机构进行相关要求的检测、监测、抽查、验证等。

4.5 处置措施

a）平台运营者发现生态机构存在不符合要求的行为时，应及时采取相应的处置措施，包括但不限于：应拒绝其入驻申请，通知整改、下架、删除、断开相关应用服务、冻结账号等处理措施。

b）对于存在多次违规行为的，如多次通知拒不整改的，或采用技术手段规避审核的，平台运营者应酌情采取加严处理措施，如：直接下架、冻结账号等。

4.6 申诉投诉

平台运营者应建立完善用户举报投诉处置等措施，对生态机构及时进行跟踪监测及处理违法违规行为。

a）平台运营者应提供用户反馈渠道，建立用户投诉、举报、评论处理流程，对用户反馈存在的问题进行验证，如确认存在问题的，应及时采取处理措施。

b）平台运营者应向生态机构说明本文第 4.3 节（4.3 安全评估）所采取的措施及具体理由，并提供申诉渠道，及时处理生态机构对审核结果的异议。

c）平台运营者应建立侵权投诉受理流程，提供侵权投诉渠道，依照《民法典》等相关法律法规要求履行通知义务，并根据受理流程或法院判决采取必要的处理措施。

5 生态机构安全要求

5.1 基本要求

a)生态机构应满足网络安全等级保护安全要求，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理、安全运维管理等要求。具体参照 GB/T 22239-2019《网络安全等级保护基本要求》。

b）生态机构应建立相应的安全组织，指定安全负责人，负责日常安全事件响应与应急处置；

c）应建立必要的安全管理制度，在研发、生产、办公及业务运营等环节规范安全行为，保障业务及系统的信息安全。

d）生态机构应对员工（含外包）录用前，进行必要的背景调查，并对关键岗位人员签署关于安全保密的责任协议。

e）生态机构应在员工调岗或终止劳动合同时，及时调整或终止权限，强化终端及平台管控等，避免数据及个人信息产生泄漏。

5.2 网络安全管理

5.2.1 网络与系统安全

a）应对登录系统的用户分配帐号和权限，并重命名或删除默认帐号，修改默认帐号的默认口令。

b）应制定明确的密码策略，确保设备帐号的密码规则满足策略要求，禁止使用空口令或默认口令，定期更换密码，帐号初始密码禁用固定密码，应随机生成。密码强度要求满足包含字母大写、字母小写、数字、特殊字符其中的三种或以上组合，且长度至少 8 位以上。

c）应及时删除或停用多余的、过期的帐号，避免帐号多人流通。

d）业务系统应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

5.2.2 安全运维管理

a）应用、系统、数据库等重要信息系统，应做日志记录并保存，以支持有效的审核、安全取证分析等。

b）应建立安全应急处置机制，制定安全事件应急预案，发生安全事件时能及时启动应急响应机制，进行风险排查处置，采取措施防止危害扩大，并上报处置结果。

c）生态机构应向平台提供完整的机构基础信息、包括但不限于涉及相关业务资产清单（应用名称、服务器 IP 等）、安全负责人信息（姓名、手机、邮箱等），如有变更须在规定时间内完成信息更新。

d）生态机构应参与平台组织的安全能力评估工作，也可自行提交由第三方安全机构完成的安全评估，安全评估需提交平台运营者审核，审核通过后视为有效。

5.3 数据安全管理

5.3.1 管理制度

a）生态机构应建立专门的数据安全组织，指定数据安全负责人，负责数据安全相关的日常安全事件响应与应急处置。

b）应建立必要的数据安全安全管理制度，在研发、生产、办公及业务运营等环节规范数据安全行为，保障业务及系统的数据安全。

5.3.2 数据生命周期管理

a）应采用合法合规手段进行数据收集，应对外部数据来源的合法性进行确认，确保数据的合法性和正当性。

b）应采用安全通道、通道加密、数据加密等措施保护数据，如：HTTPS、VPN 等，宜采用国家密码管理部门认证的加密算法及认证产品，如：SM2、SM3 等。

c）应采用加密方式对相关数据进行存储。

d）生态机构向其他数据处理者提供、委托处理数据的，应当通过合同等与数据接收方约定处理目的、方式、范围以及安全保护义务等，并对数据接收方履行义务的情况进行监督。

e）涉及数据跨境业务，应遵循国家数据跨境相关的法律法规。

f）涉及数据销毁时，应采取有效技术手段进行完全删除，确保数据不可恢复。

5.4 隐私安全管理要求

a）应建立个人信息管理制度，包括但不限于个人信息处理规则、使用规范、安全保护措施、处理个人信息主体询问的渠道和机制、个人信息处理人员的行为要求等。

b)收集个人信息应遵循最小必要原则，并向个人信息主体明确告知收集的个人信息类别，并获得个人信息主体的明示同意后，方可进行信息收集；向个人信息主体提供更正或补充个人信息的方法。

c）应以清晰明了易理解的方式，向用户展示收集个人信息的处理目的、处理方式、授权字段。

d）变更原先的处理目的、处理方式、授权字段、授权框唤起场景或其他超出用户已授权范围的，应当在使用用户信息前重新取得用户授权。

e）不得在非必要采集用户信息的环节，要求用户提供个人信息，或要求用户授权非使用服务必要的额外信息。

f）不得在用户进行授权时违反相关隐私保护合规要求，造成隐私违规，相关情形包括但不限于：过度授权、捆绑授权、强制授权、授权叠加、授权弹窗打扰、重复授权、授权环节死循环导致用户无法退出等用户信息授权问题。

g）个人信息数据收集中包含人脸、人声等敏感个人信息的，应取得个人单独授权同意，并保留个人信息主体授权文件。

h）应对个人敏感信息进行加密存储和传输。

i）生态机构应当在特定情形下主动删除个人信息，这些情形包括处理目的已实现、无法实现或不再必要，以及停止提供产品或服务等，用户完成注销操作后应即时删除或匿名化账户内的个人信息。

j）应建立个人信息保护投诉、举报机制，提供投诉、举报渠道，及时受理、处理和反馈处理结果；不得在采集用户信息后，通过线下、电话、短信等营销方式触达用户，造成用户打扰和投诉。

k）应与个人信息处理岗位人员签署个人信息安全保护责任书。

5.5 内容安全管理

5.5.1 内容安全

a）应遵守国家法律法规，以及国家的政策制度要求。

1)不应发布与宪法所确定的基本原则不符，危害国家安全，损害国家利益的内容。

2)不应发布破坏国家统一，破坏民族团结，破坏国家宗教政策以及宣传邪教和破坏民族团结的内容。

3)不应发布法律、行政法规禁止的其他内容。

b）遵守社会公共秩序，以及社会道德和公序良俗，确保发布的信息真实可靠有出处。

1)不应散布谣言，扰乱社会秩序，破坏社会稳定的内容。

2)不应散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的内容。

c） 遵守平台规则，维护公平公正的经营环境，确保各方的合法权益。

1)不应发布恶意攻击平台、损害经营环境或者不正当竞争的内容。

2)不应发布侮辱、诽谤或者损害他人合法权益的内容。

3)不应发布涉及个人隐私的内容，包括客户电话、地址等有关内容。

5.5.2 产品及服务安全

a）生态机构应遵守明码标价等相关规定，明示收费标准、收费方式，明示内容应真实准确、醒目规范，扣费前需经用户确认，不应存在恶意收费行为，如：未在商品购买和商品支付界面向用户进行二次确认等。

b）若生态机构服务存在自动续费功能，应清晰明示费用明细、使用条件等信息。

c）生态机构产品的付费使用条件应与明示的信息一致，不应在付费后仍存在其他未明示的使用条件。

d）生态机构应保证价格透明公开一致。

e）生态机构应遵循应用营销推广的相关法律法规，禁止出现绝对化表述。

f）生态机构需确保商品及服务信息描述，满足真实性、完整性、一致性的要求。

g）生态机构应遵循平台运营者的商品管理规范要求，不得经营法律法规禁止或平台禁止经营的业务内容。

5.6 资金安全管理

5.6.1 管理制度

a）应设立专门的资金管理部门。

b）应建立明确的资金管理制度。

c）应定期向监管部门及平台运营者报告资金管理情况（资质、身份凭证、交易意图等）。

5.6.2 账户管理

a）为客户开立账户时， 应核对客户有效身份证件，并留存有效身份证件的复印件或者影印件。

b）应建立用户身份验证机制，确保交易双方身份真实可靠。

c）应设立专门的资金存储账户、确保用户资金的独立性。

d）应定期对资金账户进行对账，确保账目清晰准确。

5.6.3 交易管理

a）需对资金的往来进行实时监控，发现异常交易及时进行干预。

b）定期进行内部资金审计，确保资金管理合规。

d）应采用加密技术保护用户的资金安全，防止信息泄露。

e）用户提现时需核实用户身份信息，确保请求的真实性。

f）用户提现流程应简化，禁止设置不必要的流程。

g）禁止私自挪用用户资金。

5.6.4 风险防范

a）应建立资金风险预警机制，及时发现并处理风险。

b）应积极配合监管及平台机构核查相关资金动向，及时跟进处置相关问题。

c）应建立用户反馈渠道，及时处理用户上报的资金安全问题。

d）定期开展员工培训，提高员工的资金安全风险防范意识。

附 录 A
（资料性）
生态机构安全分级认证规则

表A.1给出了生态态机构安全分级认证的规则主要围绕安全要求、安全过程、安全等级三个维度展开：

a）安全要求维度

安全要求维度明确了生态机构在安全保护领城应符合的要求,包括网络安全、数据安全、隐私安全、内容安全、资金安全。

b）安全过程维度

安全过程主要明确了生态机构在各个阶段应达到的安全管控水位，主要包括风险管理、风险响应、安全意识、安全能力、经营健康。

c） 安全等级维度

生态机构安全等级划分为五级，具体包括：1级是基础合规级,2级风险可控级，3级是组织保障级，4级是自主防护级，5级是持续优化级。

安全等级	共性特征	说明
一级 基础合规级	生态机构在安全过程中不能有效的执行相关工作，仅在部分业务执行过程中满足基本的底线安全合规要求	被动的响应安全过程
二级 风险可控级	生态机构建立了基本的应急联络、安全响应、消费者投诉处理等流程	建立基本的安全风险响应机制
三级 组织保障级	生态机构建立安全管理组织，并制定了有效的组织制度，相关人员具备相应的安全能力，能够有效的保证机构及业务的安全。	在组织级别实现了安全过程的规范执行
四级 自主防护级	生态机构具备有效的安全能力建设，能够主动的进行定期的自我安全检测、红蓝攻防演练、漏洞扫描等。	建立了主动的安全防护能力
五级 持续优化级	生态机构制定了出于持续改进状态下的安全目标，寻找改进的机会，并对组织的安全规程进行持续改进。	根据组织的整体目标不断的改进和优化安全过程

表A.1生态态机构安全分级认证规则

参 考 文 献

[1] GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求
[2] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[3] GB/T 40050-2021 网络关键设备安全通用要求
[4] GB/T 20988-2007 信息系统灾难恢复规范