TC260-PG-20263A

网络安全标准实践指南

——互联网平台新型腐败预防和处置要求

v1.0-202602

全国网络安全标准化技术委员会秘书处

2026 年 2 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：中国电子技术标准化研究院、北京京东世纪贸易有限公司、中央网信办（国家网信办）数据与技术保障中心、国家计算机网络应急技术处理协调中心、北京三快科技有限公司

本文件主要起草人：胡影、郝春亮、陈舒、任英杰、井奇、李爽、王志伟、张震、田喜清、王寒生、王俊

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国刑法》《中华人民共和国公司法》《中华人民共和国劳动法》等法律法规，指导互联网平台企业开展内部人员新型腐败问题预防和处置工作，制定本文件。

本文件规定了预防和处置互联网平台人员新型腐败的基本要求、日常防范要求和处置要求。本文件适用于预防和处置互联网平台人员发生的流量操控、数据舞弊、权限寻租、榜单造假等新型腐败问题。

目　录

1 范围

本文件规定了预防和处置互联网平台人员新型腐败的基本要求、日常防范要求和处置要求。

本文件适用于预防和处置互联网平台人员发生的流量操控、数据舞弊、权限寻租、榜单造假等新型腐败问题。

2 术语定义

2.1 互联网平台人员新型腐败

指互联网平台企业从业人员，利用职务或工作便利，借助系统权限、数据资源、流量资源等平台技术资源，谋取不当利益的违法违规行为，简称“新型腐败”。

注：新型腐败的表现方式主要包括流量操控、数据舞弊、权限寻租、榜单造假等。

3 基本要求

互联网平台企业应开展内部人员新型腐败问题的预防和处置工作，基本要求如下：

a) 定期排查新型腐败问题或隐患，包括但不限于：

1) 流量操控：通过虚假注水、恶意劫持、暗箱干预等手段扭曲正常流量分配规则的行为；

2) 数据舞弊：非法数据爬取、敏感数据倒卖、算法参数篡改等数据滥用行为；

3) 权限寻租：利用系统管理权限违规开展账号权限交易、审核权限变现等行为；

4) 榜单造假：通过技术手段或人工干预制造虚假热度，影响热搜榜单、商品排名等展示的行为。

b) 设立廉洁部门，承担统筹、监督和执行企业内部廉洁工作的职责，明确企业主要负责人为廉洁工作负责人；

c) 建立健全廉洁制度体系，明确与数据、流量、权限相关的廉洁要求，明确廉洁管理责任分工，建立各部门及岗位的廉洁管理责任清单，通过企业公告或制度文件明确内部人员廉洁约束要求；

d) 明确权限管理策略及内部审核流程，使用统一权限管理平台进行员工权限管理，确保内部人员只能访问与其职责相关的数据和系统，并定期对账号权限进行审查，及时清理超范围授权，确保权限使用合理；

e) 强化技术防控能力，利用大数据、人工智能等技术构建智能化新型腐败风险防控体系，实时监控数据访问、流量分配、权限操作等关键环节，发现异常及时预警并反馈处置情况；

f) 建立便捷、安全的举报渠道，鼓励内部人员、用户及合作伙伴举报疑似新型腐败行为，及时处理举报线索并向举报人反馈结果；

g) 定期开展全员廉洁教育培训与廉洁文化宣传，通过案例分

析、情景模拟等形式提升员工廉洁意识和职业道德，营造廉洁文化氛围。

4 日常防范要求

4.1 业务流程审查

互联网平台企业应保证每年至少开展一次业务流程审查，重点针对流量分配、权限管理、广告投放等高风险场景，识别可能导致内部人员发生新型腐败风险的漏洞，并及时整改，确保业务流程符合廉洁制度要求。

4.2 日常风险防控

互联网平台企业应开展常态化日常风险防控工作，要求如下:

a) 明确数据监控策略并充分识别数据异常行为，通过风险监测、数据防泄露等技术手段对数据处理异常行为进行监测、预警、拦截;

b) 利用技术手段对流量分配进行监控，及时发现异常波动并分析人为操纵可能性，保障业务相关算法的公平与透明。

4.3 定期开展审计

互联网平台企业应每年至少开展一次审计工作，要求如下:

a) 定期对新型腐败进行审计，涵盖数据访问、流量分配、权限管理、广告投放等高风险场景;

b) 定期对算法模型进行审计，防止通过不正当手段操控算法以

获取不公平的资源倾斜；

c) 对审计发现的系统权限、数据资源、流量资源等平台技术资源违规访问行为，特别是流量操控、数据舞弊、权限寻租、榜单造假等，应及时开展调查。

5 处置要求

5.1 事件分级

互联网平台企业应在发现有关情况或接到有关线索后，通过查阅文件、人员访谈、调取日志等手段进行调查取证并对取得的证据进行分析，确定内部人员是否存在新型腐败行为以及新型腐败行为的性质。新型腐败行为事件按照危害对象（国家安全、公共利益、企业利益、个人利益）和危害程度（高、中、低）可分为特别重大事件、重大事件、较大事件和一般事件。新型腐败行为事件分级参考见本实践指南附录A。

5.2 处置

5.2.1 较大事件和一般事件处置

经调查内部人员确有新型腐败行为，但未达到立案追诉标准的，互联网平台企业可采取以下措施：

a) 要求违规人员作出检讨并留存相关记录，并重新开展廉洁教育培训；

b) 扣减违规人员的绩效分数或绩效奖金等经济处罚措施；

c) 对违规人员进行警告、降职、撤职、解除劳动合同等相应处分。

5.2.2 特别重大事件和重大事件处置

经调查内部人员新型腐败行为已达到立案追诉标准的，互联网平台企业应：

a) 暂停涉事人员职务及系统权限，保护现场证据；

b) 整理完整证据链（财务记录、系统日志、证人证词等），移交公安机关，并指定专人配合调查，定期跟踪案件进展。

附录 A

（规范性）

新型腐败行为事件分级参考

按照危害对象（国家安全、公共利益、企业利益、个人利益）和危害程度（高、中、低），新型腐败行为事件可分为特别重大事件、重大事件、较大事件和一般事件。

a）对国家安全产生高、中程度影响，或者对公共利益产生高程度影响的新型腐败行为事件，认定为特别重大事件；

b）对国家安全产生低程度影响，对公共利益产生中程度影响，或者对企业利益、个人利益产生高程度影响的新型腐败行为事件，认定为重大事件；

c）对公共利益产生低程度影响，或者对企业利益、个人利益产生中程度影响的新型腐败行为事件，认定为较大事件；

d）对企业利益或个人利益产生低程度影响的新型腐败行为事件，认定为一般事件。