ICS 35.240.01
CCS L69

T/CCIASC

团 体 标 准

T/CCIASC 0007—2024

移动游戏业务安全实施要求

Practice Requirement for Business Security of Mobile Games

2024－08－09 发布　　2024－08－16 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。

本文件由深圳市腾讯计算机系统有限公司提出。

本文件由中国计算机行业协会归口。

本文件起草单位：深圳市腾讯计算机系统有限公司、中国软件评测中心（工业和信息化部集成电路与促进中心）、广东省游戏产业协会、三七互娱网络科技集团股份有限公司、深圳市创梦天地科技有限公司、深圳雷霆信息技术有限公司、深圳市迷你玩科技有限公司、天翼安全科技有限公司、中国联合网络通信集团有限公司。

本文件主要起草人：李长江、王岳、韩萌、鲁晓昆、林丽、邓晓玉、谢尧裕、李鑫、张旭、王翔、周杰、宋舸、程露萍、安健、张学扬、陈天成、蔡依然、和森、洪其限、金莎、刘博文、罗平、王荣富、袁方、郑海涛、叶明亮、黄峻峰、王丽娜、王校杰、谢晓勇、周祺、康和、李朝霞、杨志。

移动游戏业务安全实施要求

1 范围

本文件提出了移动游戏业务安全的服务能力架构并规定了移动游戏业务安全的实施要求，包括：通用措施、事前防范措施、事中应对措施、事后处置措施以及多方协同措施。

本文件适用于移动游戏开发商、移动游戏运营商、移动游戏安全服务商、云服务提供商以及终端厂商，为移动游戏业务安全的实施提供重要的参考依据。

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 32414-2015《网络游戏安全》

GB/T 32413-2015《网络游戏外挂防治》

T/CADPA 7.1-2020《网络游戏术语 第1部分：游戏类别》

T/CADPA 7.2-2020《网络游戏术语 第2部分：研发》

T/CADPA 7.3-2020《网络游戏术语 第3部分：运营》

3 术语和定义

GB/T 32414-2015、T/CADPA 7.1-2020界定的以及下列术语和定义适用于本文件。

3.1

移动游戏 mobile games

通过移动网络，用户利用移动终端(例如：手机、掌机、PAD等) 进行操作的游戏。

注：不包含国产小程序网络游戏。

3.2

移动游戏业务安全 business security of mobile games

在移动游戏运营过程中，移动游戏的客户端、服务器及信息系统抵御意外事件及恶意行为的能力，以及保障用户游戏安全权益的能力。这些事件和恶意行为将危及游戏运营所依赖的软件或数据，并进一步对游戏的平衡性、可用性等造成严重影响。

3.3

加固 hardening

通过对游戏核心代码加密、关键资源保护及针对性反调等方式，防止游戏包体被分析和破解的安全技术。

3.4

外挂 cheat

指游戏用户通过采取特定作弊工具实现无敌、锁血、自瞄、飞天、透视、改伤害等功能，从而影响游戏平衡性的问题。

3.5

反外挂 anti-cheat

指用于检测和防止玩家使用作弊工具的技术和措施，旨在保护游戏的公平性和平衡性。

3.6

内容安全管理 in-game content moderation

针对游戏内的承载媒介（例如：文本、图片、音频和视频）涉及的内容安全问题进行管理，包括：涉黄、涉诈、涉政、涉暴、涉辱骂、涉敏感内容以及其他违法违规内容等。

3.7

游戏经济系统安全管理 in-game economy risk management

针对黑产团伙通过大量账号和第三方工具，获取、转移、售卖游戏资源或提供服务引发的问题进行管理。可能引发的问题包括：游戏资源超发，游戏经济系统遭到破坏等。

3.8

用户游戏安全权益保障 user rights for game security

指游戏用户在游戏安全维度上应当享有的权利或利益，游戏开发商或游戏运营商或游戏安全服务商应通过管理机制和技术能力保障用户取得这些基本权益内容，主要包括：处罚后权益保障、举报权益保障、游戏账号及虚拟财产安全权益保障等。

4 移动游戏业务安全服务架构

4.1 概述

移动游戏业务安全的服务能力应基于游戏所遇到的安全问题而生并不断发展，最核心的安全服务能力包括：加固、反外挂、内容安全管理、游戏经济系统安全管理和用户游戏安全权益保障。移动游戏业务安全实施包括：通用措施、多方协同措施、事前防范措施、事中应对措施和事后处置措施。移动游戏业务安全服务能力和安全实施架构如图1所示。

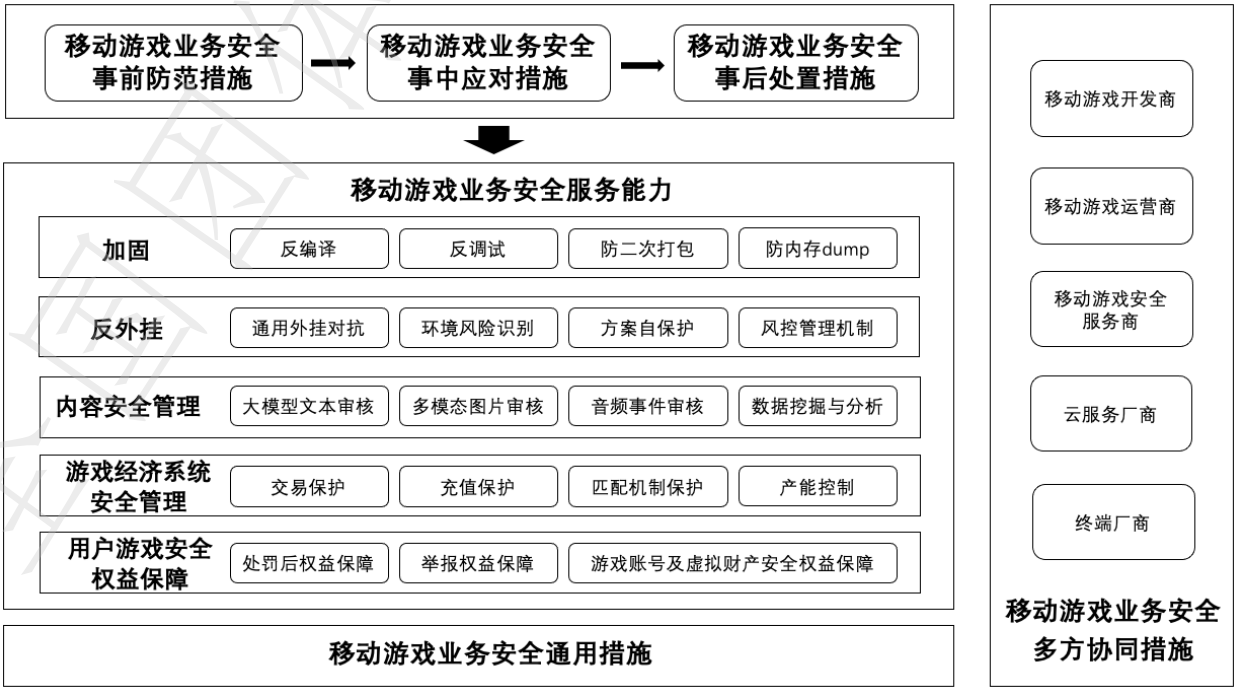

图1 移动游戏业务安全服务能力和安全实施

4.2 加固

加固技术主要包括以下4大类：

a) 反编译：作弊用户会使用例如：IDA Pro等反编译工具对游戏核心代码进行静态分析，再根据分析结果制作游戏的外挂和破解版。通过对游戏核心代码的加密对抗这类反编译行为，从而达到提高外挂制作门槛，延缓破解包出现的目的。游戏的核心代码大多数存于native端，即编译后是Elf文件格式的.so文件。游戏代码加密主要针对.so文件的.text段、.rodata段等关键信息加密；

b) 反调试：作弊用户除了静态分析游戏代码外，还可以通过动态调试的方法，在游戏运行时进行调试，从而获取他们制作外挂和破解版所需的信息。反调试可以阻止恶意玩家通过逆向工具动态调试游戏进程；

c) 防二次打包：游戏的破解版即是二次打包游戏包体后的产物。游戏的破解包有无需root，安装方便等利于传播的特性，若无防二次打包功能，破解版包极容易成为分布最广的外挂载体，因此提高破解版包出现是安全方案的重头。防二次打包需要做到阻止作弊用户在修改apk包体内受保护的文件后重新打包的行为，从而使破解版产生的门槛提高，延缓破解版出现的时间；

d) 防内存dump：针对常用的游戏引擎，游戏包体内会有相应的符号信息文件，例如：globalmetadata.dat，作弊用户通过内存dump该文件并结合二进制文件，例如：libil2cpp.so可以还原游戏符号信息。因此防内存dump也是一种安全方案。防内存dump需要能加密关键信息文件，并能防御市面上常见开源的dump工具。

4.3 反外挂

反外挂技术主要包括以下4大类：

a) 通用外挂对抗：通用外挂包含修改器、变速器、虚拟机等可以对游戏实施作弊功能的应用，此类外挂的特点是免费使用、易上手、传播广泛、与游戏客户端功能无关。反外挂SDK最基础的功能就是需要检测和对抗此类的外挂样本，打击这些广泛传播的外挂样本，提高外挂作弊的门槛；

b) 环境风险识别：用户除了使用通用外挂之外，还会使用一些存在作弊风险的设备，包括：模拟器、刷机设备、root设备，这些设备本身可能不具备作弊的功能，但是作弊用户可以在此类设备的基础上结合第三方插件、模块完成作弊行为。环境风险识别可以用于区分正常用户的设备和存在作弊风险的设备，游戏客户端可以根据此类数据区分有风险和无风险的用户；

c) 方案自保护：反外挂方案的存在是为了在游戏客户端不做变更的基础上大幅提高对外挂和可疑行为的检测能力，在一些极端的外挂对抗环境下，部分外挂会攻击反外挂安全方案，导致安全方案不能按照原有的功能正常实施。因此反外挂方案对自身的保护能力就显得十分重要。安全方案对于自身的保护能力和抗分析能力可以有效阻止外挂剥离、攻击外挂检测，包括反调试功能、安全方案完整性校验、安全方案心跳机制等等；

d) 风控管理机制：由于反外挂方案是运行在游戏客户端为主，自身会包含一些在游戏客户端实施的打击和对抗功能，例如：游戏客户端内部弹窗提醒、游戏客户端主动退出等，为了防止安全方案可能产生对正常玩家和正常游戏行为的误判，以及潜在的方案稳定性问题，反外挂安全方案应具备良好的风控机制，可以动态的调整自身的运行逻辑和打击阈值，降低安全方案对游戏本身的风险。

4.4 内容安全管理

内容安全管理主要包括以下4大类：

a) 大模型文本审核：指通过使用大型机器学习模型提升原有审核技术方案的能力，建立自动审核和筛选文本内容的过程。这种技术可以用于识别和过滤掉不适当、有害或违反游戏安全准则的内容。大模型文本审核的主要优点是能够处理大量的文本数据，而且速度快，效率高。但也存在挑战和限制。例如，机器学习模型可能会误判一些内容，或者无法理解一些复杂的语境和含义。因此，大模型文本审核通常需要不断优化和调整模型，以提高其性能和准确性。

b) 多模态图片审核：多模态图片审核是指对包含多种媒体类型（如图像、文本、音频、视频等）的内容进行审核和分析的过程。在多模态图片审核中，主要关注的是对图像内容的审核和分析。融合了视觉和文本指令等多模态输入，借用大数据预训练技术，显著提升对复杂场景和任务的理解

及生成能力，具备更高的泛化性。多模态图片审核旨在识别和过滤出违规、不当或有害的图像内容，以保护用户免受不良内容的影响。

c) 音频事件检测：是指对音频信号进行分析和处理，以识别和检测特定的音频事件或声音类型的技术。音频事件可以是各种声音，如说话、音乐、环境噪声、交通声等。音频事件检测技术的目标是从音频信号中自动识别和分类不同的音频事件，以提供对音频内容的理解和分析。这项技术在许多应用领域中都有重要的应用，如语音识别、音乐分类、环境监测、声音事件分析等。

d) 数据挖掘与分析：是指应用数据挖掘和分析方法来处理和分析用户自生成内容的数据，以从中提取有用的信息和知识。数据挖掘是一种从大规模数据集中自动发现模式、关联和趋势的技术。在自然语言处理中，数据挖掘技术可以用于文本分类、情感分析、实体识别、关系抽取等任务。通过应用数据挖掘技术，可以从文本数据中发现隐藏的模式和规律，帮助理解文本内容、提取关键信息和进行预测。数据分析是对数据进行系统性研究和解释的过程。在自然语言处理中，数据分析技术可以用于统计分析、语言模型建立、语义分析等任务。通过数据分析，可以对文本数据进行统计描述、模型建立和推理，从而获得对文本数据更深入的理解和洞察。数据挖掘与分析技术在内容安全技术中的应用非常广泛。它们可以帮助处理大规模的数据，提取有用的信息和知识，并支持各种任务的实现和改进。这些技术可以通过机器学习、统计分析、挖掘算法等方法来实现，以提高对数据的理解和应用能力。

4.5 游戏经济系统安全管理

游戏经济系统安全管理主要包括以下4大类：

a) 交易保护：通过干扰黑产在游戏内交易系统进行资源转移，从而压制黑产盈利；

b) 充值保护：通过监控充值货币在游戏内转移情况从而进行管控，例如：配合退款、黑卡充值、渠道充值等数据；

c) 匹配机制保护：通过降低团伙使用第三方工具卡匹配进去同一局，从而压制卡匹配作弊行为;

d) 产能控制：通过灵活控制黑产账号获取资源比例，从而压制黑产规模。

4.6 用户游戏安全权益保障

用户游戏安全权益保障主要包括以下3大类：

a) 处罚后权益保障：游戏用户因为被处罚而自然产生的基本权利，如处罚知情权、处罚申诉权等，游戏开发商或游戏运营商或游戏安全服务商应当通过技术手段以及建立相关的流程、机制等来满足这些权益内容；

b) 举报权益保障：游戏用户针对游戏环境中的各类违规行为而行使的监督或反馈权利，游戏开发商或游戏运营商或游戏安全服务商应提供具体的方法、工具或能力等满足用户的举报诉求，同时应基于客观、公正、统一的原则进行及时核实处理；

c) 游戏账号及虚拟财产安全权益保障：游戏开发商或游戏运营商或游戏安全服务商应当通过管理机制或技术能力满足用户在游戏场景下的账号登录、核心功能使用以及虚拟财产交易/转移等操作时的安全诉求，如开展风险警示，提供登录辅助验证手段，支持用户被盗申诉，提供敏感操作限制等。

5 移动游戏业务安全通用措施

移动游戏开发商和运营商应实施以下通用措施：

a) 组织制度管理：加强组织管理，制定内部安全规范策略，建立符合组织的安全管理制度，建立风险管理、安全审计管理、各类应急响应方案机制；

b) 人员管理：定期对相关员工进行安全培训，包括安全意识培训、安全技术培训、安全操作规范培训、安全红线宣传、个人信息保培训等，合理确定个人信息处理的操作权限；

c) 文档管理：对各阶段生成的安全相关文档进行管理，包括：安全需求说明，风险评估报告，安全设计、应急方案等文档；

d) 数据管理：根据业务场景构建数据安全能力，降低业务数据被篡改、泄露、损毁或者丢失等风险；建立数据保护相关的管理制度和技术措施。

6 移动游戏业务安全多方协同措施

6.1 移动游戏开发商

移动游戏开发商在游戏开发过程中，应采取关键逻辑在服务端进行校验、通信协议加密等手段提升游戏被攻击、篡改的门槛，同时宜在游戏上线前进行中专业的漏洞挖掘，并提前修复。移动游戏开发商应针对破解版、外挂、内容安全、经济安全等问题接入成熟、稳定的自研或第三方专业安全组件。

6.2 移动游戏运营商

移动游戏运营商应在移动游戏上线前确保已接入必要的安全方案，且对接入安全方案后的游戏进行全面的测试以确保其稳定性。在移动游戏运营过程中应及时、有效地进行安全运营，例如：对外挂作弊玩家进行处罚，对恶意用户自生成内容内容及发布者进行处理等。

6.3 移动游戏安全服务商

移动游戏安全服务商应为移动游戏提供专业的安全方案。在方案研发层面，应将方案对移动游戏的性能影响降至最低，并确保安全方案所涉及到的组件、接口已经过充分的稳定性、兼容性测试。在数据层面，应确保相关数据的收集、存储、处理均符合合规要求，并通过相关协议文件向合作的移动游戏开发商或移动游戏运营商公开。在游戏运营阶段，安全服务商所提供的方案应具备完善的容灾、风控机制。

6.4 云服务厂商

云服务厂商应为移动游戏提供安全可信的云计算服务，针对性防范拒绝服务攻击、数据泄露等安全问题，确保云平台服务的网络安全及系统安全，保障云平台的安全、稳定运行。同时，服务器应进行安全加固，设计弹性伸缩和灾备切换的系统，安装DDoS高防服务。对于使用自有机房的场景，也需要做好上述相关安全防范。

6.5 终端厂商

终端厂商应为移动游戏提供硬件安全和系统安全保障，应确保用户在体验移动游戏服务过程中的系统稳定性，确保移动游戏服务的持续性和流畅性。终端厂商应满足移动游戏使用流程的业务需求和高效协同，提供必要的协助，不应以欺骗、误导、强迫等方式影响移动游戏用户的选择，不应以弹窗、文字、按钮、设置风险检测、验证等方式干扰、破坏或者妨碍移动游戏用户下载、安装、升级、使用移动游戏服务，限制移动游戏用户使用推送通知功能。同时，终端厂商应需秉承公平、公正的原则，不根据移动游戏开发商、移动游戏运营商、移动游戏来源等因素设置不同的机制，避免干扰移动游戏的正常运行过程。

7 移动游戏业务安全事前防范措施

7.1 加固

7.1.1 安全评审

在移动游戏上线前，移动游戏开发商应对移动游戏的安全性，主要包括：动态注入攻击风险、篡改和二次打包风险和核心so文件被逆向分析风险等进行评估，对移动游戏版本进行漏洞挖掘及风险评估，并对潜在的漏洞和风险进行修复，并准备应急预案。

7.1.2 游戏代码加固

移动游戏开发商应对移动游戏代码和资源等应进行加密和保护，防止客户端代码和资源被破解、调试等，提高静态分析门槛，以此延长客户端被破解的风险。

7.1.3 稳定性和兼容性测试

移动游戏在上架之前，移动游戏开发商应对游戏包体针对主流移动终端机型进行稳定性和兼容性测试。测试通过后，可将移动游戏包体对外发布。

7.2 反外挂

7.2.1 安全评审

在移动游戏上线前，移动游戏开发商和游戏运营商应对移动游戏的安全性，主要包括：游戏客户端的反调试、反通用外挂、可疑环境检测、代码混淆、实时对抗能力、游戏逻辑漏洞、游戏协议加密等方面等进行评估，对游戏版本进行漏洞挖掘及风险评估，并对潜在的漏洞和风险进行修复，并准备应急预案。

7.2.2 客户端加密和反外挂方案接入

为了提升客户端安全性，移动游戏开发商和游戏运营商和游戏安全服务商应对客户端代码、组件和资源等进行加密和保护，防止其被破解或调试。对于外挂风险较高的游戏，应要求接入外挂检测方案，以便在游戏运营期间检测和打击外挂和作弊用户。

7.2.3 准备处置手段

为了及时处理作弊玩家和外挂问题，移动游戏开发商和移动游戏运营商应在运营前准备相应的处罚方案，主要包括：封号、踢下线、禁止模式等。同时，我们应提高游戏或重点模式，例如：核心玩法、排位天梯、多人竞技、排行榜的准入门槛，例如通过大数据模型识别小号或历史作弊号，禁止其进入，并实行实名认证等措施来预防外挂行为。同时，移动游戏客户端方案和封号策略应具备稳定的风控能力，避免安全方案自身上线后产生大面积误报影响正常用户的游戏体验。

7.3 内容安全

7.3.1 制定内容安全技术方案

移动游戏开发商和移动游戏运营商宜形成一套自我审查，自我约束的基本准则，包括：检测能力基线、处罚能力基线、人工审核能力基线、产品功能形态基线等等，从而保障发布的移动游戏产品具备统一的违规信息内容检测能力与检测机制，方便安全部门统一指挥，统一部署，最大化提升企业对违规信息审查的效力。

7.3.2 发布防骗公告

移动游戏运营商应在游戏内外官网论坛等适合场景处，滚动提示玩家注意防范，积极警示引导玩家提高自我安全意识，提高防诈意识，了解相关法律法规，避免上当受骗，从而对自身与财产安全造成不必要的损失，同时鼓励玩家在游戏中，积极对破坏游戏发言环境的行为做斗争。

7.3.3 建立突发事件预警响应机制

移动游戏安全服务商应建立健全重大或突发事件预警响应机制，保障重大事件发生时，能快速制定相关标准，高效部署最新违规信息检测能力，协调人工审核人力与审核占比，建立专项应对的数据监控，保障游戏发言环境和谐稳定。

7.4 游戏经济系统安全

7.4.1 游戏经济系统评审

在游戏上线前&游戏新玩法上线前，移动游戏安全服务商应对经济系统详细评估，深度挖掘可能存在的黑产风险玩法，包括玩法风险、BUG风险等，在不影响正常玩法的前提下，给出相应的改进建议，优化游戏玩法，提升自身的安全性，提前降低黑产风险。

7.4.2 潜在黑产问题分析

针对存在用户与用户、用户与系统之间可以相互交易、转移游戏资源的游戏，移动游戏运营商应监控游戏内黑产团伙规模，黑产如何获取、转移、售卖游戏资源。

针对存在渠道分红的游戏，移动游戏运营商应监控渠道构建虚假帐号、恶意自充值等行为，利用游戏渠道买量和分成规则，进行牟利的黑产团伙。

针对存在玩家特殊需求的游戏，移动游戏运营商应监测玩家特定需求类型，黑产提供相应服务所引发的问题，主要包括：破坏游戏公平性，影响用户的移动游戏体验等

7.4.3 经济系统安全管控方案部署

针对不同移动游戏的不同黑产问题，移动游戏运营商和移动游戏安全服务商应制定相应的管控目标，深入结合该移动游戏的特点和需求，部署经济系统的安全管控方案，降低黑产影响，提高移动游戏口碑。

7.5 用户游戏安全权益保障

7.5.1 明确处罚证据类型要求

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应当在游戏发行前明确处罚证据类型。证据类型应包括：游戏行为数据、发言文字、昵称、图片、音频、视频等不同证据类型，能够有效提供违规行为所发生的时间、游戏账号、游戏角色、游戏场景等基本信息。

7.5.2 实现处罚证据存储能力

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应当在游戏发行前实现处罚证据存储能力，应针对游戏账号、游戏角色开展的违规行为检测、处罚活动中应提前建立并验证相关证据的采集和存储能力；应保证相关证据信息得到完整妥善保存，且不可篡改，例如：可结合可信存证的区块链服务开展证据存储工作；处罚证据在处罚有效期内应妥善保存，宜采用永久保存机制。

7.5.3 实现游戏安全信息的触达能力

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应当在移动游戏发行前实现移动游戏安全信息的触达能力。应建立例如：移动游戏客户端内部弹窗或者移动游戏客户端内部通知邮件等机制的游戏安全信息触达能力，用于移动游戏运营过程中的处罚、举报、游戏账号、游戏内财产风险等信息触达场景使用；同时宜建立更贴近用户使用习惯的非游戏渠道信息触达能力，例如：基于短信或者微信等平台的消息推送等。

7.5.4 设置举报入口

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应当在游戏发行前设置举报入口，并满足如下要求：

a) 举报功能应覆盖个人资料、会话发言、组织资料、对局、图片、文本展示、自定义玩法展示等基本场景，并在对应场景设置明显的举报入口；
b) 举报面板应支持用户确认被举报者昵称、选择举报原因，同时宜提供用户进一步补充举报信息的能力；
c) 举报原因应基于游戏品类以及具体场景进行合理设计，其中针对用户自生成恶意的举报原因宜包含言语辱骂、色情低俗、政治敏感、欺诈、非法信息等选项。

7.5.5 实现举报数据接入

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应当在游戏发行前实现举报数据接入，并满足如下要求：

a) 用户举报数据应包含：举报者信息、被举报者信息、举报来源、场景信息、举报原因、举报描述、必要证据信息，例如：用户自生成发言内容、用户昵称头像信息等，用于后续的举报核查处理以及进度通知和查询等；
b) 举报数据应至少保存半年以上。

7.5.6 实现账号恶意注册防护能力

账号恶意注册通常包括：恶意批量注册、虚假注册信息等情况。移动游戏运营商应当对恶意注册的行为或结果进行识别，如提前建立基于账号注册行为和账号注册环境数据的识别能力；同时移动游戏运营商应在账号和游戏角色的注册场景中内置有效的人机对抗或身份核验方式来避免恶意注册行为的发生，如短信验证码、动态验证码（例如：滑块、选择图片、算数等）、三要素身份核验等。

8 移动游戏业务安全事中应对措施

8.1 加固和反外挂

8.1.1 建立安全运营体系

移动游戏开发商在获得反外挂检测数据后，应在游戏服务器上建立一套完整的安全运营体系，包含作弊监控体系、实时检测体系、作弊处罚体系以及客观衡量游戏安全性的指标体系。通过对作弊玩家数据的持续监控，及时发现并应对作弊行为。同时制定多样化处罚策略，根据作弊行为的严重程度进行相应处罚，例如断开链接、分级封号等措施。

8.1.2 制定反外挂策略

在运营过程中，移动游戏运营商和移动游戏安全服务商应实时关注游戏安全系统数据，对异常游戏行为、外挂黑模块等制订反外挂策略，及时利用处置手段处罚异常用户。定期回顾检测效果，确保反外挂的打击效果。

8.1.3 核实外挂舆情

移动游戏运营商应对外挂信息进行定期摸排，关注外挂论坛和玩家举报，及时安排团队成员测试和确认所获信息。确认外挂情况属实，应立即将其列入应对计划，确保对抗效果。

8.1.4 定期发布反外挂效果

基于日常运营外挂对抗情况，移动游戏运营商应梳理反外挂运营措施和外挂打击效果，定期通过官方渠道发布相关信息，以提升用户对安全建设的参与度和感知。

8.1.5 多渠道挖掘外挂线索

移动游戏运营商和移动游戏安全服务商应利用技术手段和社工手段，记录有价值的外挂作者线索信息，以备后续跟进法律途径打击。

8.2 内容安全

8.2.1 建立违规信息检测机制

移动游戏运营商和游戏安全服务商应共同健全用户注册、账号管理、信息发布的实时审核、跟帖评论审核、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度，并采用人工智能审核系统，可依托深度学习等算法，实现内容，行为，画像多维度协同，高效准确识别移动游戏中出现的文本、图片、视频、语音等多种媒体的违规内容，对敏感信息、色情低俗、消极谩骂、广告、拉人、违法违规等多个类型的自动识别。同时风控系统宜采用人机协同的方式识别恶意内容，对于智能AI审核系统的正向反馈至关重要。应在这个过程中不断刷新对这些非结构化恶意的认知，并升级恶意内容的判定基准与自动审核能力。

8.2.2 及时阻断违规信息传播

移动游戏运营商和游戏安全服务商应将检测到的违规信息实时拦截，有效阻断恶意信息的曝光，根据处罚制度，对于发布违规信息的账号处以禁言或封号的处罚，避免对正常用户造成干扰，保障健康的移动游戏内发言环境。

8.2.3 精细化游戏场景控制违规信息

移动游戏运营商应根据移动游戏产品用户生成内容场景繁多、信息内容呈现形态多样的特点，细化昵称、消息、好友私聊、游戏社区、搜索等场景的安全策略和机制，精准打击移动游戏内各场景的违规信息，以降低误判和漏判的风险，提升用户的游戏体验。

8.2.4 建立应急响应与监控

移动游戏运营商应在安全运营流程上进行两个环节的监控。其一，在违规信息的传播环节中，对其发展趋势进行监控，以随时感知违规信息状态；其二，在对违规信息处置的环节中，对违规信息是否已经被处置做出监控，以确保处置是切实有效的。当监控预警发生时，应配备应急响应的移动游戏运营人员，以及时对问题进行处理，保障安全运营的效果。

8.3 游戏经济系统安全

8.3.1 精准识别黑产账号

游戏安全服务商应对黑产数据进行实时监控，包括对游戏内黑产账号进行实时监控（宜识别游戏中95%以上的黑产账号）和对游戏内黑产交易进行实时监控（宜识别游戏中95%以上的黑产交易），更精准地检测黑账号并监控黑产交易，为移动游戏运营商在对黑产用户帐号和黑产交易进行处置时，有充分的依据。

8.3.2 实施管控方案

移动游戏安全服务商应搭建线下黑产规模大盘，将黑产规模映射到现实货币进行数字量化，让移动游戏运营商可以从宏观层面把握游戏黑产的规模，同时进行管控之后，也能直观地看到经济挽回的效果。

8.4 用户游戏安全权益保障

8.4.1 举报的处理与反馈

移动游戏开发商或移动游戏运营商或移动游戏安全服务商对举报进行处理与反馈要求如下：

a) 针对用户举报单应及时开展举报核查工作，被举报账号或角色确实存在违规行为的应进行处理，同时将处理结果及时通知举报者；
b) 针对用户自生成内容的举报，例如：政治敏感、欺诈、非法信息等，应基于举报证据信息尽快完成核查工作，宜在24小时内完成；
c) 应建立有效的举报通知渠道，对举报者及时反馈举报进展或举报核查结果信息；同时宜提供便捷的举报查询工具，支持用户查询其历史举报记录。

8.4.2 账号及虚拟财产的风险控制

移动游戏运营商/安全服务提供商应针对不同风险类别建立消息提醒、消息警告等对用户有效的触达能力，对于已经明确的高风险虚拟财产交易、转移操作宜建立及时干预或制止的能力。其中风险主要包括：游戏账号的异常登录相关类别，如异地登录、高危环境登录、新设备登录等，以及游戏账号可疑被盗等情况，同时，风险宜包括账号长期未改密、大额交易、频繁敏感操作与高风险账号进行交易等。

8.4.3 账号登录保护

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应提供游戏账号登录过程中的必要保护能力，例如：账户密码登录、游戏平台授权游戏登录、扫码授权登录等方式。宜提供短信、token验证、常用设备验证、人身核验等不同的登录辅助验证方式。

8.4.4 敏感操作限制

移动游戏开发商或移动游戏运营商或移动游戏安全服务商宜针对游戏内财产交易、财产转移、道具分解或遗弃等敏感操作提供基于辅助验证手段的功能限制与解除能力，从而保障用户虚拟财产安全。辅助验证手段可以采用如短信、token验证、常用设备验证、人身核验等不同的验证方式。

9 移动游戏业务安全事后处置措施

9.1 加固和反外挂

9.1.1 用户运营

移动游戏运营商和游戏安全服务商应针对不同类型的用户采取不同的运营手段，进一步巩固加固和反外挂运营的效果。

9.1.2 技术运营

移动游戏运营商应对安全检测方案进行持续迭代升级，保持对更新外挂的持续检测和打击的技术能力。

9.1.3 舆情运营

移动游戏运营商和游戏安全服务商应保持对外挂渠道、黑产信息的摸排和监测，并及时采取有效措施应对。

9.1.4 法律途径

移动游戏运营商应通过司法机关，对影响较大的并可溯源的外挂进行刑事打击，对外挂作者的违法行为进行追究和索赔。

9.2 内容安全

9.2.1 违规信息举报和处理机制

移动游戏运营商和游戏安全服务商应建立完善的移动游戏举报机制，为用户提供用户自生成内容场景中，例如：文字、图片、实时语音、语音消息等内容的规范举报服务。应采用人机协同高效全面地覆盖举报信息处理，并在游戏内外渠道向举报者反馈处理结果，实现举报、处理、反馈的用户服务闭环。

9.2.2 违规信息追溯能力

由于自动化审核技术与审核人员对于新出现的违规信息与变种内容在认定标准与技术迭代上存在一定的滞后性，违规信息的完全实时筛查难度巨大，故建立针对存量信息的回溯追查能力是必要的。在运营过程中，历史存量信息一经发现恶意内容，移动游戏运营商和游戏安全服务商应及时清除违规，消除影响，并更新检测标准，迭代自动化审核技术，同时对审核人员加强培训，对剩余存量信息进行统一回溯清理。

9.2.3 人工巡查机制

移动游戏运营商应针对移动游戏内用户自生成内容场景定期进行人工巡查，巡查场景包括：游戏外官网论坛以及游戏社区评论等。安全管理员应在发现违规信息后及时处置，并实时反馈给运营团队，同时完善整体审核机制的正向反馈。

9.3 游戏经济系统安全

9.3.1 事后处罚方案

移动游戏安全服务商应对购买黑产资源、黑产道具以及黑产服务的用户，进行事后教育、惩罚等措施，正向引导用户养成良好的游戏习惯。

9.3.2 人工巡查机制

移动游戏安全服务商应针对游戏内黑产场景，定期核查第三方交易平台，主播，多人群等黑产盈利方式，发现新的盈利方式，应及时处置并迭代黑产检查模型，完善整体管控机制。

9.3.3 直播平台和第三方交易平台等处理机制

移动游戏运营商应与直播平台和第三方交易平台合作，关闭违规直播间及店铺，减少黑产的传播途径，共同引导用户养成良好的游戏习惯。

9.4 用户游戏安全权益保障

9.4.1 处罚信息的触达与查询

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应提供处罚信息的触达与查询，并满足以下要求：

a) 信息完备性：应包含被处罚的账号、角色、大区、处罚方式、开始时间、周期、违规行为、处罚原因说明等必要基本信息，信息方便读取，易于理解且无异议；
b) 信息触达及时性：提高处罚信息对用户触达的及时性，例如：可采用伴随处罚下发的游戏客户端内实时触达；如涉及到非账号封禁类的功能限制处罚，应在处罚周期内每次用户能感知到功能禁止的场景中进行及时告知；
c) 信息触达方式：应实现游戏客户端内部实时处罚弹窗、游戏客户端内部通知邮件等必要手段，同时宜提供更丰富的多渠道信息触达能力，如短信、微信等信息平台的消息推送能力等；
d) 应支持用户在游戏官网开展处罚查询操作，同时宜建立专门的游戏安全服务入口，例如：游戏运营商安全中心等；
e) 应在用户授权的基础上保障游戏客户服务对相关处罚信息的获取能力。

9.4.2 处罚申诉

移动游戏运营商应针对用户提交的处罚申诉需要，移动游戏运营商应提供客服受理、处理能力，同时宜在处罚查询场景中满足用户开展自助申诉或处罚减免申请的需要；处罚申诉的处理过程宜在144小时内完成。

9.4.3 场景限制与解除

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应支持场景限制与解除，并满足以下要求：

a) 应在用户每次触发游戏功能限制时告知用户相关游戏功能受限的原因，并提供清晰明确的解除手段或引导说明；
b) 解除手段应基于最小必要性原则进行设计并操作便捷，可通过例如：短信验证、必要信息补充、人身核验等手段。

9.4.4 被盗申诉

移动游戏开发商或移动游戏运营商或移动游戏安全服务商应支持被盗申诉，并满足以下要求：

a) 应对用户提供账号被盗后的申诉服务，用于被盗账号的找回、可能涉及的账号处罚解除，同时宜提供虚拟财产受损部分的可能补偿；
b) 被盗申诉应在72小时内完成。

参 考 文 献

[1] 2023 年，腾讯游戏安全、广东省游戏产业协会、腾讯安全、伽马数据、DataEye 发布《游戏安全白皮书-2023》

[2] 2022 年， 腾讯游戏安全、广东省游戏产业协会、腾讯安全发布《游戏安全白皮书-2022》