ICS 33.050
CCS M 30

团　体　标　准

T/TAF 156—2023

云游戏安全通用技术要求

General technical requirements for cloud game security

2023-04-26 发布　　2023-04-26 实施

电信终端产业协会　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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、深圳市腾讯计算机系统有限公司、中国联合网络通信有限公司、百度在线网络技术（北京）有限公司。

本文件主要起草人：刘小丽、袁琦、党受辉、滕勇、胡飞雄、徐志桐、王海棠、郭建领、郑江林、聂蔚青、邓样辉、李大伟、王永乐、张金发、王昱龙、王伟珣、张海永、施红军、王曜。

引　　言

随着移动互联网技术的快速发展，游戏业务得到迅速发展，近期云游戏作为一种新的业务模式应运而生。云游戏以云计算为基础的游戏方式，通过将游戏运行在云端服务器上，把游戏渲染出来的的音视频画面，通过流的形式传送到终端。云游戏在基础设施安全、网络安全、云平台安全、应用安全、客户端APP安全、内容安全、数据安全和运维管理安全方面存在风险，因此需要制定相应的技术要求提高云游戏的安全能力。

本文件规定了云游戏安全通用技术要求，并结合行业的实际情况和需求编写而成。

云游戏安全通用技术要求

1 范围

本文件规定了云游戏安全通用技术要求，包括云游戏安全架构、基础设施安全、网络安全、云平台安全、应用安全、客户端 APP 安全、内容安全、数据安全和运维管理安全等。

本文件适用于云游戏开发者、运营者、分发者等进行云游戏安全设计与评估。

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。

YD/T 3228—2017 移动应用软件安全评估方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

基础设施安全 infrastructure security

运行的各类物理及虚拟资源的安全。

3.2

云平台安全 cloud platform security

基于硬件的服务，提供计算、网络和存储能力的安全。

3.3

内容安全 content security

文本、图片、视频和音频中有色情低俗、涉政暴恐、垃圾广告、不良场景等内容安全。

3.4

运维管理安全 operation management security

运行保障工作中与安全运行密切相关的管理安全。

4 缩略语

下列缩略语适用于本文件。

APP：应用程序 (Application)

VLAN：虚拟局域网 (Virtual Local Area Network)
VXLAN：虚拟扩展局域网 (Virtual Extensible Local Area Network)
GRE：通用路由协议封装 (Generic Routing Encapsulation)

5 云游戏安全通用技术要求

5.1 云游戏安全框架

云游戏安全框架见图1。

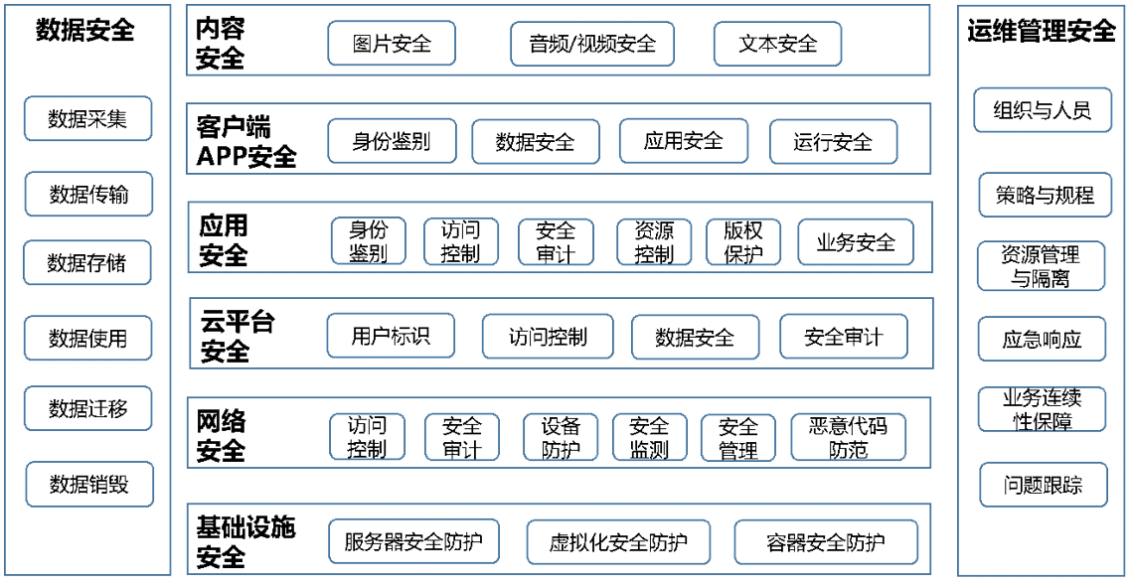

图 1 云游戏安全框架图

云游戏安全通用技术要求主要在基础设施安全、网络安全、云平台安全、应用安全、客户端APP安全、内容安全、数据安全和运维管理安全等方面规定了安全技术要求，具体如下：

a) 基础设施安全是指运行的各类物理及虚拟资源的安全。
b) 网络安全是指网络系统的硬件、软件及其系统中的数据安全，不受偶然的或者恶意的原因而遭到破坏、更改、泄露。
c) 云平台安全是指平台核心功能（如开发工具、微服务组件库等）及其运行支撑环境、资源部署管理等的安全。
d) 应用安全是指应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃。
e) 客户端 APP 安全是指客户端 APP 在运行过程中可能带来不同程度的风险或危害，如隐私窃取、远程控制等。
f) 内容安全是指文本、图片、视频和音频中内容安全，其不包含色情低俗、涉政暴恐、垃圾广告、不良场景等安全威胁。
g) 数据安全是指在数据采集、传输、存储、迁移以及销毁阶段的数据安全。
h) 运维管理安全主要是指运营管理在组织与人员、策略与规程、资源管控与隔离、应急响应与风险评估、业务连续性保障、问题跟踪与证据收集等方面的安全。

5.2 基础设施安全技术要求

5.2.1 服务器安全防护

5.2.1.1 身份鉴别

身份鉴别要求包括但不限于：

a) 应对登录服务器的用户进行身份标识和鉴别；
b) 服务器管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
c) 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施；
d) 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；
e) 当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取。

5.2.1.2 访问控制

访问控制要求包括但不限于：

a) 应采用技术措施对允许访问服务器的终端地址范围进行限制；
b) 应关闭服务器不使用的端口，防止非法访问；
c) 应基于白名单机制检测非法运行的进程或程序；
d) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
e) 应基于白名单机制限制远程管理服务端口的访问来源，防止非法访问。

5.2.1.3 安全审计

安全审计要求包括但不限于：

a) 审计范围应覆盖到服务器上的每个用户；
b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件；
c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
d) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
e) 审计记录留存时间不少于 6 个月；
f) 应能够根据记录数据进行分析，并生成审计报表；
g) 应保护审计进程，避免受到未预期的中断。

5.2.1.4 资源控制

资源控制要求包括但不限于：

a) 应根据安全策略，设置登录终端的会话数量；
b) 应根据安全策略设置登录终端的操作超时锁定；
c) 应对重要服务器进行性能监测，包括服务器的 CPU、硬盘、内存、网络等资源的使用情况，发现异常情况提供告警，并进行相应处置。

5.2.1.5 恶意代码防范

恶意代码防范要求包括但不限于：

a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
b) 应支持对防恶意代码的统一管理。

5.2.1.6 入侵防范

入侵防范要求包括但不限于：

a) 所使用的操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新；
b) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
c) 应支持对数据库攻击行为进行检测和防护；
d) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

5.2.2 虚拟化安全防护

5.2.2.1 虚拟机安全

虚拟机安全要求包括但不限于：
a) 应支持虚拟机之间、虚拟机与宿主机之间的隔离；
b) 应支持虚拟机部署防病毒软件；
c) 应具有对虚拟机恶意攻击等行为的识别并处置的能力；
d) 应支持对虚拟机脆弱性进行检测的能力；
e) 应支持虚拟机的安全启动。
f) 应保证虚拟机迁移过程中数据和内存的安全可靠，保证迁入虚拟机的完整性和迁移前后安全配置环境的一致性；
g) 应确保虚拟机操作系统的完整性，确保虚拟机操作系统不被篡改，且确保虚拟机实现安全启动；
h) 应对虚拟机镜像文件进行完整性校验，确保虚拟机镜像不被篡改；
i) 应提供最新版本的虚拟机镜像和补丁版本；
j) 应支持发现虚拟机操作系统漏洞的能力，支持漏洞修复。

5.2.2.2 虚拟网络安全

虚拟网络安全要求包括但不限于：
a) 应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机与外部网络之间的安全访问控制；
b) 应支持采用 VLAN 或者分布式虚拟交换机等技术，以实现网络的安全隔离；
c) 应采用 VxLAN、GRE 等手段支持不同租户之间的网络流量隔离；
d) 应支持东西向网络引流、网络安全编排、网络流量可视化。
e) 应支持对虚拟网络的逻辑隔离，在虚拟网络边界处实施访问控制策略；
f) 应对虚拟机网络出口带宽进行限制；
g) 可支持用户选择使用第三方安全产品。

5.2.2.3 虚拟化平台安全

虚拟化平台安全要求包括但不限于：
a) 应保证每个虚拟机能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机；
b) 应保证不同虚拟机之间的虚拟CPU指令隔离；
c) 应保证不同虚拟机之间的内存隔离，内存被释放或再分配给其他虚拟机前得到完全释放；
d) 应保证虚拟机只能访问分配给该虚拟机的存储空间（包括内存空间和磁盘空间）；
e) 应对虚拟机的运行状态、资源占用等信息进行监控；
f) 应支持发现虚拟化平台漏洞的能力，支持漏洞修复；

g） 应支持平台内采用的PKI、SSL认证等各类数字证书的统一管理，支持用户按需更换。

5.2.3 容器安全防护

容器安全要求包括但不限于：

a） 应支持容器之间、容器与宿主机之间的资源隔离；
b） 应保证容器镜像迁移过程中数据安全传输，保证迁入容器镜像的完整性和迁移前后安全配置环境的一致性；
c） 应确保容器镜像的完整性，确保容器镜像不被篡改，且确保容器镜像实现安全启动；
d） 应对容器镜像文件进行完整性校验，确保容器镜像不被篡改，确保容器安全启动；
e） 应部署一定的访问控制安全策略，以实现容器之间、容器与宿主机平台之间、容器与外部网络之间的安全访问控制；
f） 应具备容器平台漏洞的发现能力，支持漏洞修复的更新；
g） 应提供最新版本的容器镜像和升级版本。

5.3 网络安全技术要求

5.3.1 网络拓扑结构

网络拓扑结构要求包括但不限于：

a） 应绘制与当前运行情况相符的网络拓扑结构图；
b） 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
c） 应保证接入网络和核心网络的带宽满足业务高峰期需要；
d） 应根据平台服务的类型、功能及租户的不同划分不同的子网、网段或安全组；
e） 应按照用户服务级别协议的高低次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护高级别用户的服务通信。

5.3.2 访问控制

访问控制要求包括但不限于：

a） 应在（子）网络或网段边界部署访问控制设备并启用访问控制功能，或通过安全组设置访问控制策略；
b） 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力；
c） 应实现对HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制。

5.3.3 安全审计

安全审计要求包括但不限于：

a） 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行日志记录；
b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 应保证所有网络设备的系统时间自动保持一致；
d） 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
e） 应能够根据记录数据进行分析，发现异常能及时告警，并生成审计报表。

5.3.4 恶意代码防范

恶意代码防范要求包括但不限于：

a） 应对恶意代码进行检测和清除；

b） 应周期性地维护恶意代码库的升级和检测系统的更新；
c） 宜向用户提供开启/关闭某一应用获取设备级可变设备识别码的途径。

5.3.5 网络设备防护

网络设备防护要求包括但不限于：
a） 应对登录网络设备的用户进行身份鉴别；
b） 应对网络设备的管理员登录地址进行限制；
c） 网络设备用户的标识应唯一；
d） 身份鉴别信息应具有复杂度要求并定期更换；
e） 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃取；
f） 应对网络设备进行分权分域管理，限制默认用户或者特权用户的权限，做到最小授权。

5.3.6 网络安全监测

网络安全监测要求包括但不限于：
a） 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行监测，识别和记录异常状态；
b） 应根据用户需求支持对持续大流量攻击进行识别、报警和阻断的能力；
c） 应监视是否对平台服务存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
d） 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
e） 应周期性地对攻击、威胁的特征库进行更新，并升级到最新版本；
f） 应支持对违法和不良信息或非法域名的检测发现并告警；
g） 应支持对攻击行为进行分析，明确攻击目标范围，并协助回溯到攻击源头；
h） 应在网络边界处部署异常流量和对未知威胁的识别、监控和防护机制，并采取技术措施对网络进行行为分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

5.3.7 网络安全管理

网络安全监测要求包括但不限于：
a） 应确定安全管理等级和安全管理范围；
b） 应制定有关网络操作使用规程和人员出入机房管理制度，制定网络系统的维护制度和应急措施等。

5.4 云平台安全技术要求

5.4.1 用户标识

为保障云游戏平台内部的安全性，平台应对平台用户进行标识：
a） 平台应为每个管理员规定与之相关的安全属性，包括：管理角色标识、鉴别信息、隶属组、 权限等；
b） 平台应提供使用默认值对创建的每个管理角色的属性进行初始化的能力；
c） 平台应保证任何平台用户都具备唯一的标识，用户标识与产品自身审计相关联，并在产品的生命周期内唯一。

5.4.2 平台访问控制

为保障云游戏平台的安全性，平台访问控制应满足如下要求：

a) 平台应制定数据分类分级访问控制策略，应进行分类分级标识，并规定访问者对数据的访问规则；
b) 平台应对数据导出的终端、平台或个人进行身份认证；
c) 通过远程手段管理时，平台应当采取加密形式保证会话内容只被授权用户获取；
d) 平台应该基于白名单限制仅允许安装授权的应用程序；
e) 平台应该具备国家要求的反沉迷机制，对终端、个人接入进行反沉迷保护。

5.4.3 平台数据安全

为保障云游戏平台的安全性，平台应采用安全机制保证平台数据的安全：

a) 平台应对数据进行基础的安全检测；
b) 平台应采用技术手段，保证用户数据完整性、保密性和不可篡改性，防止用户信息、游戏过程、存储数据等被篡改；
c) 平台数据存储和传输应具备静态脱敏、动态脱敏和去标识化的能力；
d) 应具备防御网络攻击等安全机制；
e) 平台应采用技术手段，保证用户登录过程的鉴权信息安全传输，登录请求需加以签名校验，避免伪造登录信息造成任意账户登录或者账户之间的越权问题；
f) 平台应采用技术手段，保证支付信息的完整性、真实性以及时效性，避免造成伪造支付成功（如伪造身份、伪造人脸识别信息等）、二次支付扣费、支付金额溢出漏洞等问题。

5.4.4 安全审计

为保障云游戏平台的安全性，平台应具备安全审计能力：

a) 平台应对可审计事件生成审计记录，如平台用户的登录和注销、资源访问、对平台用户角色 的操作等；
b) 平台应采用技术手段，保证审计数据完整性、保密性和不可篡改性；
c) 平台应允许授权管理员创建、存档、删除和清空审计记录；
d) 平台应使存储于永久性审计记录中的所有审计数据可为人所理解；
e) 除了具有明确访问权限的授权管理员之外，平台应禁止所有其他用户对审计日志的访问。

5.5 应用安全技术要求

5.5.1 身份鉴别

身份鉴别要求包括但不限于：

a) 应采用两种或两种以上组合的鉴别技术来进行身份鉴别；
b) 应采取有效机制与技术手段，防止游戏串号，游戏本身可能存在盗号风险；
c) 建议游戏运营商和游戏开发商协调，提供统一的实名认证接口，避免用户重复实名认证，提高云游戏用户的体验。

5.5.2 访问控制

访问控制要求包括但不限于：

a) 应严格限制用户的访问权限，按安全策略要求控制用户对业务应用的访问；
b) 应严格限制应用与应用之间相互调用的权限，按照安全策略要求控制应用对其他应用里用户数据或特权指令等资源的调用；

c） 应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证一种身份鉴别机制是不易伪造的；
d） 应具备防范暴力破解等攻击的能力。

5.5.3 安全审计

安全审计要求包括但不限于：
a） 审计范围应覆盖到用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
b） 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
c） 应定期针对审计日志进行人工审计；
d） 应支持按用户需求提供与其相关的审计信息及审计分析报告。
e） 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能；
f） 应具备自动化审计功能，监控明显异常操作并响应；
g） 应能汇聚服务范围内的审计数据，支持第三方审计。

5.5.4 资源控制

资源控制要求包括但不限于：
a） 应限制对应用访问的最大并发会话连接数等资源配额；
b） 应提供资源控制不当的报警及响应；
c） 应在会话处于非活跃一定时间或会话结束后终止会话连接。

5.5.5 版权保护

从云游戏代码开发阶段、发行阶段、平台集成适配阶段、商业运行阶段，都实施和保障有云游戏版权保护，功能但不限于：
a） 云游戏发行方应对云游戏程序包体实施加密、加固或签名；
b） 云游戏运营平台和服务平台应保护云游戏程序包体不被泄露、破解；
c） 云游戏运营平台只有得到合法授权后，游戏才可以运行，同时实施对游戏的版权或使用规则的管理；
d） 游戏运营平台应该具有防盗链功能，确保只有经过运营平台认证、登录后的消费者才可以玩游戏。

5.5.6 业务安全

云游戏的业务安全要求包括但不限于：
a） 应支持对消极比赛、代打、演员等恶意游戏行为的举报、监控以及惩罚机制；
b） 应支持对云游戏外挂行为的监控、识别、打击以及惩罚机制。

5.6 客户端 APP 安全技术要求

客户端APP安全应满足YD/T 3228—2017第1级、第2级、第3级、第4级和第5级的要求。

5.7 内容安全技术要求

内容安全要求包括但不限于：
a） 应对图片内容进行审核，准确识别图像中的涉政敏感人物、暴恐元素、涉黄等内容；
b） 应对文本内容进行审核，有效识别涉黄、涉政、广告、辱骂、违禁品和灌水等文本内容；
c） 应对视频内容进行审核，能够识别色情、广告、违禁等视频；

d) 应对音频内容进行审核，能够识别色情、娇喘、敏感和其他违规语音。

5.8 数据安全技术要求

5.8.1 数据采集阶段

数据采集阶段安全保护要求包括但不限于：

a) 数据采集时，应标记数据的敏感度等级；
b) 数据采集方应向数据提供方告知数据的去向及用途。

5.8.2 数据传输阶段

数据传输阶段安全保护要求包括但不限于：

a) 应采用技术措施保证鉴别信息（指用于鉴定用户身份是否合法的信息，如用户登录各种业务系统的账号和密码、服务密码等）传输的保密性；
b) 应支持用户实现对关键业务数据和管理数据传输的保密性；
c) 应能够检测到数据在传输过程中完整性受到破坏；
d) 应能够检测到数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

5.8.3 数据存储阶段

数据存储阶段安全保护要求包括但不限于：

a) 应在保证密码算法安全性的前提下为用户提供对密码算法、强度和方式等参数进 行配置的功能；
b) 应提供有效的磁盘保护方法或数据碎片化存储等措施，保证即使磁盘被窃取，非法用户也无法从磁盘中获取有效的用户数据；
c) 应能够检测到数据在存储过程中完整性受到破坏，防止数据被篡改、删除和插入等操作。在数据完整性遭到破坏时，应提供授权用户可察觉的告警信息；
d) 应提供数据本地备份与恢复功能，全量数据备份至少每周一次，增量备份至少每天一次，或提供多副本备份机制；
e) 备份数据应与原数据具有相同的访问控制权限和安全存储要求；
f) 应能够检测到数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
g) 应支持用户选择第三方加密及密钥管理机制对重要业务系统数据进行加密；
h) 应提供有效的虚拟机镜像文件加载保护机制，保证即使虚拟机镜像被窃取，非法用户也无法直接在其计算资源上进行挂卷运行；
i) 应建设生产备份中心和同城灾备中心，即双活中心。双活中心应具备基本等同的业务处理能力并通过高速链路实时同步数据，日常情况下可同时分担业务及管理系统的运行，并可切换运行，灾难情况下应支持灾备应急切换，保持业务连续运行；
j) 应建立异地灾难备份中心，提供异地实时备份功能，配备灾难恢复所需的通信线路、网络设备和数据处理设备等，利用通信网络将数据实时备份至灾难备份中心。

5.8.4 数据使用阶段

数据使用阶段安全保护要求包括但不限于：

a) 应对数据的使用进行授权和验证；

b） 应确保数据仅在云游戏业务功能范围内使用；
c） 应对重要业务系统运行数据的使用进行审计，并形成审计日志，审计日志留存时间不少于 6 个月；
d） 应支持数据使用过程中的动态脱敏。

5.8.5 数据迁移阶段

数据迁移阶段安全保护要求包括但不限于：
a） 应进行数据迁移前的网络安全能力评估，保证数据迁移的安全实施；
b） 应保证数据在不同数据设备之间迁移不影响业务应用的连续性；
c） 数据迁移中应做好数据备份以及恢复相关工作；
d） 数据迁移准备应制定迁移方案，并进行迁移方案可行性评估与风险评估，确定制定数据迁移风险控制措施。

5.8.6 数据销毁阶段

数据销毁阶段安全保护要求包括但不限于：
a） 应建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程；
b） 应能够提供手段协助清除因业务终止、自然灾害、合同终止等而遗留的数据，
c） 数据销毁日志的留存时间不少于 6 个月；
d） 应确保文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除；
e） 应通过提供必要的数据销毁工具等手段，确保以不可逆的方式销毁数据。

5.9 运维管理安全技术要求

5.9.1 组织与人员

云游戏的组织与人员管理工作内容应包括但不限于：
a） 设立专门的组织负责制定安全运维策略，指导安全运维管理工作；
b） 明确服务团队人员的职责分工以及联系方式；
c） 设置专职的安全运维岗位，包括但不限于：安全管理岗、基础安全运维岗、网络安全运维岗、安全攻防测试岗等；
d） 人员应具备云游戏运维相关的知识和经验；
e） 建立与安全运维相关的人员储备计划和机制；
f） 建立与安全运维相关的人员培训计划和机制；
g） 建立与安全运维相关的人员绩效考核机制。

5.9.2 策略与规程

云游戏的安全运维策略与规程工作内容应包括但不限于：
a） 制定符合云游戏战略和目标的安全运维策略，明确安全方针、目标和原则；
b） 建立并完善安全管理制度，明确组织结构、岗位职责、工作流程、奖惩措施等；
c） 建立制度执行安全检查机制；及时进行安全监测，修补安全隐患；
d） 及时进行安全服务管理制度的培训和宣贯；
e） 对制度的执行情况进行考核，纳入人员绩效；
f） 定期（年度）对策略和规程进行完善和更新。

5.9.3 资源控制与隔离

云游戏的资源管控与资源隔离工作内容应包括但不限于：

a) 建立有效的云计算资源管理与监控制度，规范服务监测的人员操作和监测指标等；
b) 建立云计算资源的配置关联和资源授权关系，并采取有效策略隔离租户间的资源；
c) 提供服务资源的监控记录，对监控记录数据进行保存，保存期符合国家法律、法规和标准的要求；
d) 建立资产管理流程，对安全保障相关软硬件资产的采购、入库、维修、借调、领用、折旧和报废等阶段进行管理，以减少资产丢失、损坏、失窃造成的业务中断；
e) 平台的服务资源应进行统一管理，集中调度，按需弹性分配资源；
f) 采用安全的资源接口协议设计，确保资源交互数据的完整性、机密性。

5.9.4 应急响应与风险评估

云游戏的应急响应与风险评估工作内容应包括但不限于：

a) 制定应急预案，并建立应急处置流程，进行应急演练和培训；
b) 定期对服务应急预案进行及时更新，原则上每年评估不少于一次；
c) 建立信息安全事件报告和通报机制，及时向用户和监管部门通报安全事件，并根据用户事先定义的规则或者以往的事故案例采取合理的应对措施；
d) 完整记录应急事件的处置过程；
e) 定期进行安全风险评估，根据评估结果制定相应的风险处理计划，风险评估的范围覆盖云游戏平台安全保障范围。

5.9.5 业务连续性保障

云游戏的业务连续性保障工作内容应包括但不限于：

a) 识别业务连续性风险，制定满足云游戏能力的业务持续性计划；
b) 明确服务连续性的保障方式，包括数据备份、同城容灾、异地容灾等；
c) 对服务连续性和服务可用性应进行监测和风险分析，记录监测和分析结果。

5.9.6 问题跟踪与证据收集

云游戏的问题跟踪和证据收集工作内容应包括但不限于：

a) 建立问题证据收集机制，并收集、保存可用作证据的事件；
b) 对发生的问题进行分析，识别仍然具有潜在威胁的问题，消除引起有关问题的原因，避免同类问题重复发生；
c) 建立与问题管理过程一致的活动，包括问题建立、分类、调查和诊断、解决、关闭等，保证问题管理过程的完整性；
d) 建立问题分类管理机制，分类应与事件的分类一致，优先级判定方式应与事件相同，但处理时限可不同，分类管理包括问题的影响范围、重要程度、紧急程度等；
e) 建立问题的导入记录机制，将问题的处理经验记录进库，为技术服务人员以后处理事件提供参考。

电信终端产业协会团体标准

云游戏安全通用技术要求

T/TAF 156—2023

*

版权所有 侵权必究

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn