



六一云合理化使用政策（AUP）

修订时间：2021 年 1 月 10 日 生效时间：2021 年 1 月 18 日

一、引言

本《合理化使用政策》（以下简称“APU”）是《六一云用户服务协议》的重要组成部分，旨在规范六一云平台用户（以下简称“用户”）在使用本平台提供的各类云计算服务时的行为与操作，确保平台的稳定性、安全性与合规性。

用户在使用六一云服务的同时，须共同遵守本政策与《用户服务协议》的全部条款。如用户违反本政策规定，六一云有权依据《用户服务协议》及本政策采取包括但不限于暂停服务、限制访问、终止账号、清除数据等必要措施，并保留依法追责的权利。

二、定义

2.1 云服务器（ECS / 轻量应用服务器） 六一云提供的弹性计算服务，用户可以根据业务需求选择不同规格的虚拟化云服务器实例进行应用部署。

2.2 物理服务器（裸金属服务器 / 单盘机） 六一云提供的独立硬件资源，用户可以独占物理资源进行高性能计算与数据存储，但通常存在更高的维护与数据安全风险。

2.3 对象存储（OSS / OBS） 六一云提供的分布式对象存储服务，用于存储和管理大量非结构化数据。

2.4 云数据库（MySQL、MongoDB、Redis 等） 六一云提供的关系型和非关系型数据库服务。

2.5 CDN / 边缘加速服务 六一云提供的内容分发网络加速服务，用于提高站点加载速度和提升网络质量。

2.6 网络产品（公网 IP、NAT、VPN、带宽等） 六一云提供的基础网络服务，用于实现资源访问与通信。

2.7 安全服务（WAF、防火墙、堡垒机等） 六一云提供的多层次安全防护服务，用于抵御外部攻击和保障数据安全。

2.8 DevOps 工具（API、CI/CD 等） 六一云提供的开发、集成和部署自动化工具，帮助开发团队提升效率。

2.9 数据与 AI 服务（大数据计算、AI 模型训练等）六一云提供的高性能计算资源，用于数据分析与人工智能应用。

2.10 SaaS 工具（云桌面、低代码、IM 等）六一云提供的按需定制的云应用服务，如在线办公、即时通讯等。

三、产品类型和禁止行为

3.1 云服务器（ECS/轻量应用服务器等）

3.1.1 禁止行为

运行非法网站、黑灰产服务、仿冒平台；

挖矿、DDoS 攻击源、控制肉鸡网络；

用于爬虫、刷量、暴力破解、模拟注册等；

蓄意绕过计费机制或大量空跑资源。

3.1.2 规范使用建议

使用 ECS 前请根据实际业务合理配置规格（CPU/内存/带宽）；

合理规划服务运行时间，及时释放临时资源；

启用防火墙、SSH 限制、入侵检测等安全策略；

对公网服务设置访问频控、异常日志报警。

3.2 对象存储（OSS/OBS 等）

3.2.1 禁止行为

上传分发涉政、涉黄、诈骗类文件或链接；

使用 OSS 作为非法 CDN、黄牛图床、盗链站点；

存储非法爬取的数据、侵犯版权的内容。

3.2.2 规范使用建议

启用访问权限控制（私有/公开读写策略）；

对外链接建议设置过期时间或签名验证；
定期清理未使用或违规内容；

结合内容审核服务进行自动化过滤。

3.3 云数据库（MySQL、MongoDB、Redis 等）

3.3.1 禁止行为

数据库被用作爬虫缓存、欺诈行为的中间层；
密码弱口令、公开 IP 暴露数据库端口；
对数据库频繁爆破连接或超高频读写。

3.3.2 规范使用建议

数据库务必开启白名单访问和强口令；
对外服务需经应用网关中转，避免直连；
使用读写分离、缓存优化应对大规模访问；
开启自动备份和 SQL 审计日志。

3.4 CDN / 边缘加速服务

3.4.1 禁止行为

为涉政、涉黄、盗版内容提供加速；
搭建钓鱼站、诱导下载站、JS 劫持服务；
CDN 被用于虚假营销、搜索引擎欺骗。

3.4.2 规范使用建议

加速内容应为静态资源或合规动态服务；
启用防盗链、防劫持、防缓存穿透机制；
定期巡查源站及缓存内容合法性；

设置带宽上限或地域访问策略。

3.5 网络产品（公网 IP、NAT、VPN、带宽等）

3.5.1 禁止行为

使用公网 IP 进行非法端口扫描、代理搭建；

VPN 节点用于翻墙、绕过审计、跳板行为；

异常带宽冲突、僵尸流量攻击平台。

3.5.2 规范使用建议

公网访问应最小化暴露端口和服务；

禁止自建绕审计代理服务或共享给他人；

配置带宽预警、访问日志和封禁策略；

实施 IP 绑定验证与 DDoS 防护配置。

3.6 安全服务（WAF、防火墙、堡垒机等）

3.6.1 禁止行为

使用安全工具反向检测平台机制；

利用 WAF 绕过目标系统防御；

模拟攻击行为测试无授权目标。

3.6.2 规范使用建议

为关键业务配置 WAF + DDoS 联防；

安全策略应分阶段测试再部署；

堡垒机操作应留痕、设定访问审批；

禁止对非自己拥有的系统使用攻防工具。

3.7 DevOps 工具（API、CI/CD 等）

3.7.1 禁止行为

API 接口暴力调用导致平台资源异常；

使用脚本模拟用户行为刷量、刷钱、刷数据；

CI/CD 频繁打包导致编排引擎过载。

3.7.2 规范使用建议

合理配置调用频率和重试机制；

设置 API 白名单和权限控制；

CICD 应基于 Webhook 自动触发、避免手工滥用；

使用监控工具检查持续集成中的异常行为。

3.8 数据与 AI 服务（大数据计算、AI 模型训练等）

3.8.1 禁止行为

利用 AI 生成涉政、涉黄、误导性内容；

自动化脚本爬取/解析用户隐私数据；

高并发计算资源占用扰乱共享调度。

3.8.2 规范使用建议

使用训练集前须确认数据合法合规；

配置 AI 资源限额，避免高峰时段排挤其他任务；

禁止模型用于攻击模拟、社工欺诈等用途；

开启异常任务终止机制，监控计算负载。

3.9 SaaS 工具（云桌面、低代码、IM 等）

3.9.1 禁止行为

云桌面用于运营黑产业务；

IM 用作垃圾广告推送平台；

将低代码工具搭建虚假商城、非法系统。

3.9.2 规范使用建议

禁止将服务开放给不明外部用户；

内容和应用需定期自查合规性；

配置登录认证、权限分层；

云桌面应限制外部拷贝、设备绑定。

四、通用行为准则

4.1 遵守国家法律法规、公序良俗

用户必须严格遵守中华人民共和国的相关法律法规，确保在使用六一云服务过程中不从事任何违法、违禁活动。此外，用户应遵守社会公德，维护平台的正常秩序和公共利益，不得进行任何危害公共安全、恶意操控平台或损害他人权益的行为。

4.2 不得进行破坏平台运行稳定性的行为

用户不得进行任何可能影响六一云平台正常运行的活动，包括但不限于攻击、植入病毒、恶意篡改、滥用功能等行为。任何试图破坏平台技术架构、影响服务稳定性的行为将受到严厉处理。

4.3 不得滥用资源影响其他用户

用户不得利用平台的资源进行任何滥用行为，例如通过不正当方式消耗平台资源，导致其他用户的服务受影响。用户应合理规划和使用资源，避免高并发、大规模攻击或非业务需求的资源占用，影响平台其他用户的正常使用。

4.4 遵守平台产品使用规范和技术限制

用户在使用六一云的各项服务时，应遵循平台产品的使用规范和技术限制。具体包括但不限于：服务的最大带宽限制、硬件资源的配置规范、存储服务的使用要求、数据传输的合规性等。用户应当了解并遵守相关规范，避免违反平台的设计和技术要求。

五、违规等级与处罚

六一云对用户在上平台发生的违规行为，采用分级管理的方式进行处理。根据违规行为的严重程度，我们将违规行为划分为**轻微违规**、**一般违规**、**严重违规**和**极其严重违规**四个等级，并对每个等级的违规行为设定相应的处罚措施。具体表格如下：

违规等级	违规行为类型	处罚措施
轻微违规	- 轻微违反服务使用规范，未导致其他用户影响	- 警告一次，要求改正； - 限制部分资源使用权限一定时间； - 提供改进建议。
一般违规	- 影响个别用户服务质量或轻微违反平台安全要求	- 限制用户部分服务的访问权限； - 暂停相关服务或资源使用 24-48小时； - 罚款（如适用）。
严重违规	- 大规模影响其他用户服务质量，违反数据保护、版权法规	- 暂停用户所有相关服务，时间可根据违规情况确定； - 罚款（如适用）； - 必须提供整改报告并经过审核； - 不得再次发生同类违规。
极其严重违规	- 大规模攻击平台、泄露用户数据、重大安全漏洞等	- 永久封禁用户账户； - 终止所有服务和资源的使用； - 对外公告，可能涉及法律诉讼或报告给相关部门； - 赔偿其他受影响用户的损失（如适用）。

5.1 违规等级说明

轻微违规

轻微违规行为通常是指用户没有恶意，但由于不当操作或管理不善，造成了平台服务的轻微问题或不符合使用规范的行为。此类行为不会严重影响平台的运行或其他用户的正常使用。

一般违规

一般违规行为可能会影响其他用户的服务质量，但不至于造成严重的影响。通常是由于违反了平台的一些中等规定，例如滥用部分资源，或违反安全要求导致系统暂时不稳定。

严重违规

严重违规行为通常会导致大范围的服务中断、平台系统受到攻击，或违反了重要的法律法规要求，例如侵犯版权、泄露数据或进行不当操作。此类行为可能会影响到大量的用户或导致平台服务的严重中断。

极其严重违规

极其严重违规行为通常是指对平台造成重大损害，可能对平台的整体安全性、用户数据保护等方面带来巨大风险或损害。此类违规行为不仅影响平台的正常运营，也可能对外界带来法律责任或信任危机。

5.2 处罚措施说明

警告：用户将收到书面警告，并告知其违规行为的严重性及改正的必要性。

限制访问权限：在一定时间内限制用户对部分服务的使用权限，如暂停访问某些敏感功能。

暂时停用服务：在违规情况下，六一云可根据违规行为的程度暂停用户的相关服务，时间可以是 24 小时至 48 小时，具体视情况而定。

罚款：对于违法行为，可能需要支付一定的罚款，金额依据违规的严重性进行判定。

永久封禁账户：对于极其严重的违规行为，六一云有权永久封禁用户账户，停止所有服务，并且采取法律行动（如适用）。

注：平台保留根据具体情况调整违规等级和处罚措施的权利，依据实际违规定义和平台运营政策，进行灵活处理。

六、违法行为与处理

六一云平台致力于遵守国家及地区的法律法规，并对涉及违法的行为进行严格的管理与处理。若用户在平台上从事违反法律法规的行为，六一云将根据相关法律法规的要求，采取相应的处罚措施，并有可能将此行为报告给相关执法部门。

6.1 违法行为类型

6.1.1 侵犯知识产权：

上传、传播、存储、分享侵犯版权、专利、商标等知识产权的内容。

使用六一云服务从事非法复制、分发软件或其他受版权保护的内容。

6.1.2 传播非法内容：

上传、传播包含政治敏感、淫秽、暴力、诈骗等违法信息的内容。

发布违反公序良俗、煽动违法犯罪、危害社会安全的内容。

6.1.3 网络攻击与数据盗窃:

利用平台资源进行黑客攻击、DDoS 攻击、网络钓鱼、入侵他人系统。

盗取、传播他人用户数据或违反数据隐私保护法规。

6.1.4 金融诈骗与非法交易:

利用平台服务进行虚假宣传、金融诈骗、非法资金募集、传销、洗钱等行为。

发布虚假交易信息, 诱导他人进行非法交易活动。

6.1.5 违法个人隐私数据处理:

擅自收集、处理、泄露用户个人隐私信息, 违反个人隐私保护相关法规。

6.2 违法行为的处罚措施

对于涉及违法的行为, 六一云将根据违规的严重程度以及相关法律法规, 采取以下处罚措施:

违法行为类型	处罚措施
侵犯知识产权	<ul style="list-style-type: none">- 停止相关服务并封禁账户;- 立即清除违法内容;- 向版权方提供违规信息并配合追责。
传播非法内容	<ul style="list-style-type: none">- 停止服务并封禁账户;- 向相关执法机构报告, 配合调查;- 清除非法内容并进行内部调查。
网络攻击与数据盗窃	<ul style="list-style-type: none">- 永久封禁账户;- 向公安机关或其他相关部门报案;- 清除相关攻击脚本、程序和非法获取的数据。
金融诈骗与非法交易	<ul style="list-style-type: none">- 暂停或终止服务, 封禁账户;- 向监管机构报告, 提供证据;- 追回非法获得的资源或收益。
违法个人隐私数据处理	<ul style="list-style-type: none">- 立即清除违规数据;- 永久封禁账户;- 向个人隐私保护监管机构报告, 配合调查。

6.3 违法行为的法律追诉

法律责任：

对于严重违法行为，六一云保留追究用户法律责任的权利，包括但不限于民事赔偿、行政处罚及刑事诉讼。

平台将依法向执法机关提供相关的证据，并配合政府部门开展调查工作。

执法协作：

六一云将在涉及违法行为时，积极配合公安机关、监管部门或其他执法机关的调查与处理。

对于被认为存在违法行为的账户，平台有权在法律允许的范围内主动协助相关部门采取调查措施。

6.4 其他合规措施

用户责任：在使用六一云平台时，用户应主动遵守国家法律法规及行业监管要求，确保所使用服务的合法性与合规性。

合规审查：平台保留定期进行用户合规性审查的权利，以确保平台的安全和合法性。

6.5 违法行为的申诉与整改

用户如认为平台对其违法行为的认定存在误判或处罚过重，可以向六一云提出申诉。平台将提供申诉通道进行核实并做出合理调整。对于已整改的违法行为，平台可考虑恢复相关服务，但必须提供合规整改报告。

备注：六一云平台将坚决打击和防范任何形式的违法行为，并严格遵守相关法律法规的要求，以维护平台的正常运营秩序与用户的合法权益。