溜云库安全白皮书

（版本 V4.0.0）

版本变更记录

日期	版本
2024 年 5 月	V4.0.0
2022 年 10 月	V3.5.0
2020 年 5 月	V3.0.0
2018 年 10 月	V2.0.0

目录

前言

深圳特鹏网络有限公司提供的 3D 溜溜网免费客户端——溜云库，提供模型库和图库下载服务，下载模型后无需解压，可直接拖入 MAX、SU 和 CAD 等软件中使用，不丢贴图；同时溜云库开发了原创材质库，涵盖常用材质，可一键拖拽使用，原创材质库为溜云库所有，帮助用户提高作图效率。

溜云库的定位为一站式素材下载管理软件，支持在线和本地素材混合式管理、企业共享素材和协同办公。其主要特点为：免解压下载素材、批量管理本地素材、从 MAX 内部把优质模型添加到本地和百万级别素材库，支持企业库管理、云渲染及各类 MAX 插件下载的功能，软件具有高度的扩展性与实用性。采用前沿技术，对产品、用户数据进行全生命周期的安全保障。

一. 安全团队及职能

溜云库作为 3D 溜溜网的客户端，一直都把用户业务和数据的安全保护列为最高优先级工作。公司具有完善的基础架构安全以及用户业务、数据安全保护体系，可以为用户提供从物理到应用层面的全方位防护。

溜云库安全团队由安全管理与合规、业务安全、数据安全、应急响应、安全工具开发团队构成。工作内容包括产品设计安全评估、代码安全审阅、漏洞扫描、渗透测试、威胁情报、入侵检测、应急响应、数据安全、安全合规等。

二.合规与隐私性

溜云库高度重视产品的合规性，积极对标国内最高标准合规性要求。目前溜云库已通过国家多项合规性认证，标志着我们在信息安全管理、服务质量管理、IT 服务管理等方面达到了更规范化、更标准化的水平，为公司全面质量体系的改进和完善奠定坚实的基础。

溜云库积极跟进国内对产品合规的要求，通过安全管理与合规团队对接各级监管机构，确保提供的产品和服务符合要求。

三.人员安全

特鹏网络建立了安全的人力资源管理流程：

• 新员工的聘任须经过人力资源专员和岗位需求部门主管的审批，新员工招聘流程与结果记录在人力资源系统中；

• 新员工录用前，人力资源部会根据岗位的重要性，并在国家法律法规允许的情况下对员工进行背景调查，确保该员工的录用符合公司的各项规章制度；

• 新员工须签订劳动合同和保密协议，其中对员工在信息安全方面所应承担的责任和义务进行了规范；

• 法务人员每年对员工保密协议和第三方保密协议的法律条款进行至少一次审阅并在需要时进行更新，更新后通过内部知识平台进行发布，以确保所有员工和相关人员可以获取最新的保密协议；

• 员工离职须由本人或部门领导在人力资源系统中发起申请，经过人力资源部、相关职能部门进行审核后方可正式离职。特鹏网络建立了完善的培训及学习体系，新员工入职后均须参加包括公司文化、规章制度、信息安全以及奖惩机制等内容的培训。

同时公司不定期针对员工的专业知识技能和信息安全意识组织培训，建立了如下培训机制：

- 公司不定期组织信息安全相关培训，增强员工的信息安全技能；
- 公司不定期举行信息安全活动，对信息安全意识进行宣贯；
- 公司不定期通过多种方式向员工传达安全意识，如制作安全意识宣传资料并通过邮件、宣传画等形式传达至员工。

四.客户端安全

4.1 运行环境安全

溜云库对运行的环境会进行严格的检测，包括越狱检测、调试检测、注入检测等，检测目的是保证客户端运行在可信任的环境中，以防程序被破解或被恶意软件所利用。

4.2 数据安全

溜云库本地信息均加密进行存储。客户端与服务器之间的全链路通信，均用 https 或 wss 进行加密。

4.3 安全漏洞防护

溜云库具有专职安全漏洞挖掘团队，对 windows 客户端进行安全评估和漏洞挖掘，同时对使用的第三方组件进行漏洞检测，尽可能发现应用程序存在的漏洞，保证客户端的安全。

五.网络安全

5.1 网络访问控制

溜云库使用公司自有设施提供基础架构服务，包括机房、传输、网络、服务器、操作系统等，并由其提供对应安全服务。在此基础上，溜云库对服务器的访问具有加强的安全控制，所有服务必须通过堡垒机进行操作并进行审计。通过白名单来控制业务服务的访问来源，保证服务只有信任来源可以访问。

5.2 DDoS 及网络攻击防御

溜云库服务通过 CDN、动态加速来为客户提供网络接入访问，并且通过公司负载均衡访问后端服务；在遇到针对机房的 DDoS 攻击时，通过网络接入服务商（如中国电信等）提供的清洗服务来进行攻击防御。

5.3 网络传输加密

溜云库在内外网均采用 HTTPS、SSL 进行传输，保证了传输过程的安全，保证信息不会被中间人篡改、窃取。

六、服务器安全

溜云库使用自有机房的物理服务器、云服务器为客户提供服务。溜云库采取了一系列安全管控措施，保障服务器生产安全，有效防范网络恶意攻击行为。

6.1 服务器访问控制

溜云库定期对服务器资产进行扫描，及时关闭非必要的端口及服务，保障对外权限最小化，过滤不安全的服务，降低安全隐患。安全人员定期进行弱口令检测，督促服务器运维人员提升密码复杂度，防范暴力破解。

6.2 漏洞扫描

溜云库采用自动化的漏洞扫描工具定期进行服务器漏洞检测，由安全人员确认后第一时间通告给相关人员进行处理修复，且运维人员会定期进行系统补丁更新，有效保障服务器稳定运行。

6.3 入侵检测

溜云库自有机房物理服务器全面部署了 HIDS（服务器入侵检测系统），可以实时监控服务器文件基线变更，发现异常进程、捕捉主动异常外连、木马后门等异常行为，并及时作出响应。安全团队会密切跟踪安全态势和最新的攻击手法，研究入侵特征，并定期升级防御策略。6.4 异常检测溜云库安全团队对服务器产生的海量主机日志进行多维度的安全分析，建立异常检测自模型，及时发现服务器上的风险操作、异常进程、恶意网络连接等异常行为，并及时作出响应。安全团队会密切跟踪安全态势和最新的攻击手法，不断迭代安全算法模型，能够更新异常行为特征，并定期升级防御策略。

七、应用安全

溜云库通过安全开发流程保证产品安全。

7.1 安全开发流程

我们力图从安全漏洞的源头控制安全隐患。所有开发人员、产品经理都要接受安全培训，了解相关的安全漏洞成因及编码知识。安全团队在项目启动时，与项目经理进行沟通，确保安全需求、安全测试在项目计划中体现。同时安全团队会怼产品使用的第三方库、工具进行评估以及漏洞挖掘，确保没有供应链引入的漏洞。安全团队会与产品团队一起进行设计和编码的安全性审阅。在产品上线前，会进行渗透测试以及部署的安全评估，来保证服务的安全性。

7.2 用户账号安全

用户对溜云库系统的访问，通过输入密码的方式来进行份的认证。溜云库接入风控与反作弊系统。具备反恶意注册、反撞库、反暴力登录破解等防护功能。用户采用密码+动态验证码验证登录，可以有效避免因密码丢失导致的账号泄露。

7.3 漏洞与安全事件管理

溜云库通过多种手段监控内、外部安全漏洞与威胁情报信息。安全团队采用自动化的安全扫描工具对自身服务、操作系统进行扫描，通过定期的渗透测试对应用系统进行安全检查。漏洞及威胁情报信息经安全团队确认后，将根据危害情况确定风险等级，并第一时间推送至相关部门进行修复处理，公司拥有完善的漏洞生命周期管理策略，专业的安全团队跟进所有安全问题的解决。

溜云库安全团队执行优秀的应急响应策略，安全事件发生时，安全团队会根据安全应急预案迅速对事件做出等级划分，并启动应急响应流程，阻止安全事件扩大。安全事件处理完成后，会对事件进行复盘，复盘内容包括事件发生的原因、事件处理的过程及结果、事件主要负责人及后续跟进措施等内容，并记录复盘结果和后续跟进措施，保障事件闭环。

八.数据安全

溜云库对数据具有完整的生命周期管理，从数据的创建、存储、传输、使用、销毁都有明确的流程和技术保障，公司拥有相应控制措施以确保数据传输、数据存储、数据访问以及数据销毁流程的安全性

8.1 数据传输

溜云库为用户提供了支持强加密协议的数据传输链路，内容拉取、身份验证、操作指令等数据传输均使用 HTTPS 进行加密。

8.2 数据存储

溜云库使用安全的密钥机制对数据进行加密存储，我们对所有内容及数据都进行了加密存储。溜云库制定了完善的数据分类分级管理办法，对用户本地素材、用户个人信息、企业台管理系统中的信息等都进行了严格的分类分级管理，并对所有系统中存储的敏感信息进行了加密处理，有效保障用户信息安全。

加密算法内嵌于源代码中；密钥由密钥管理系统（简称“KMS 系统”）产生，并由各应用调用。KMS 服务负责密钥和敏感配置信息的生命周期管理，包括创建、存储、分发、使用、更新、删除等。溜云库用户的数据加密使用的主密钥和溜云库服务的各种其他敏感信息（如数据库账户、密码等）均存储于溜云库维护的 KMS 系统中，访问需通过 KMS 接入进行。KMS 系统的主密钥使用密钥共享协议生成多份密钥分量，分发给不同职能角色进行管理，提供大于总数一半以上的密钥分量才能还原 KMS 系统的主密匙。KMS 主密钥会定期轮转

更新，提高 KMS 数据的安全性。

8.3 数据访问

用户数据的访问，均进行了严格的权限隔离。用户之间在没有授权的情况下，无法互相访问。对数据的访问必须通过数据所有者显式的授权，比如共享操作等来完成。

特鹏网络员工对用户数据的访问被严格限制和审计，员工默认没有对任何用户数据的访问权限。特殊的访问需求要经过用户的显式授权以及内部严格的审批流程，才可以获得临时访问权限，在操作完成后权限将立刻被收回。我们对数据的操作均有详细日志记录，并区分不同操作者角色，授予不同的权限。操作需要进行审批并进行审计。我们不会公开披露您的信息，除非获得您的同意。但根据法律法规、强制性的行政执法或司法要求，在必须提供您个人信息的情况下，我们可能会依据要求的个人信息类型和披露方式向行政执法或司法机构披露您的个人信息。当我们接到披露请求时，在符合法律法规的前提下，我们要求其必须出具与之相应的法律证明文件，我们仅提供执法部门因特定调查目的且有合法权利获取的数据。在法律法规许可的前提下，我们披露的文件均在加密措施的保护之下。

8.4 数据销毁

在终止对用户服务时，溜云库管理员会删除用户账户信息，在符合当地法律法规的前提下，永久删除用户数据。磁盘报废均需经过消磁处理并销毁，确保无剩余信息。企业机构的离职员工可直接退出企业。企业机构如需注销账户，联系客服可申请注销，后台将对需要注销的账号进行数据销毁。

8.5 数据安全检测

溜云库线上环境所有服务器的登录行为、操作行为、服务器安全基线文件变更、访问权限变更和数据访问行为都会被记录。我们通过建立用户行为画像和异常行为模型，实现异常行为的识别、分析和关联，自动化实时检测各种异常数据访问行为，如对数据的非法访问、恶意数据爬取和风险操作、登录异常、权限升级等，并进行告警或阻断。

九.物理基础设施安全

特鹏网络采用自有基础设施为各个地区的客户提供服务，公司制定了数据中安全管理制度，明确规定了机房访问管理、机房环境安全等要求，并采取了完善的措施保障基础设施安全。

9.1 物理访问授权

特鹏网络用自有基础设施，包括机房、传输、网络设备、安全设备、服务器等。专人负责负责溜云库基础设施的维护和安全。溜云库使用的自有机房按照 Uptime Institute Tier3 以上等级建设，达到了非常高的可用性标准。数据中心由专业人员进行日常维护，并设有实时监控。

9.2 运营管理安全

机房管理人员每月进行数据检测并形成月报，每年进行一次数据检测，检测内容包一括巡检内容包括基础建设环境管理、数据访问和权限管理及资产安全管理等，并出具检测报告，并就检测报告发现的异常及时进行处理。

十.灾难恢复与业务连续性

10.1 备份与灾难恢复

特鹏网络制定了相关规定，对相关数据的备份策略、备份数据保管和备份恢复性测试等方面进行规范。数据库均有定期快照和备份，数据两地三备份存储，同时公司部署了备份执行情况监控机制，确保数据备份的完整性。溜云库定期进行备份数据恢复性测试。

10.2 应急演练

特鹏网络具有完备的应急演练机制，定期进行故障演练，参加人员包括业务团队、安全团队、运维团队等。至少每年对可能导致业务中断的情况进行一次灾备演练以保证数据的可用性。

十一. 变更控制

11.1 程序变更

特鹏网络制定了完善的程序变更管理规定，明确了变更管理要求及流程，包括变更案方制定、变更审批及变更实施等。对线上服务的稳定性、可用性、安全性造成已知或潜在影响的操作，均属于线上变更范围。溜云库的开发严格控制变更操作，防止变更操作影响服务的稳定。线上操作必须有操作单，批准后才可进行。公司为各产品相关应用部署了独立的开发、测试及生产环境，变更操作遵守灰度发布上线，上线均需进行小流量测试，才可正式发布，以此确保服务的稳定和安全。

11.2 源代码控制 OP

溜云库制定了严格的源代码管理流程，研发人员仅可访问和管理其所属团队对应的代码仓库。代码仓库中各项目代码仓设置了代码仓负责人，研发人员如需申请其团队以外的代码仓库访问权限时，须在代码仓库中提交申请，经其部门主管和所申请的代码仓库负责人审批后，才可添加相应权限。

11.3 基础架构变更

溜云库在公网边界部署访问控制列表对网络访问进行控制。若需对 ACL 配置基线及网络访问控制列表进行变更，运维人员通过平台提交申请，由专业工程师对变更合理性进行判断后执行操作。仅授权的工程师拥有执行络访问配置的变更操作权限。

11.4 变更监控

特鹏网络每年执行内部审计以检查公司内部控制体系的运行情况，其中涵盖对变更管理相关控制的执行有效性检查，并将结果汇总在内部审计报告中。若发现异常，由内审部门和相关负责团队沟通并跟进整改结果。变更管理过程中存在不兼容职责的分离，包括变更开发、测试、批准、发布及监控。