自审制度

一、部门及人员

我司设立自审自查小组，并由以下人员组成：

自审负责人：唐儒彦

审核人员：蔡育聪、叶佳进

二、工作职责

1. 审核人员应掌握内容审核的政策法规和相关知识；

2.在任何情况下，审核人员均可在内容自审这一工作中表达其独立的审核意见；

3.审核人员须以最终保证本企业的产品和服务的合法性和合规性为目的，对在自审工作中发现违法违规的产品及服务内容进行记录并提请中止，作出提交修改，督促修改，复审等审核意见。

4.审核人员负责保管审查记录；

5.审核人员遇有对产品及服务内容的合法合规性不能准确判断的，可向广东省文化和旅游厅申请行政指导；

6.审核人员有组织内部培训工作，对企业开发、运营人员进行内容审查方面的培训的责任。

三、审核标准

未采取监管措施或未通过内容自审的动漫产品，不得向公众提供。在所有需审核人员进行自审的内容中，不得含有以下内容：

1. 反对宪法确定的基本原则的；

2.危害国家统一、主权和领土完整的；

3. 泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；

4. 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的； 宣扬邪教、迷信的；

5. 散布谣言，扰乱社会秩序，破坏社会稳定的；

6. 宣扬淫秽、赌博、暴力或者教唆犯罪的；

7. 侮辱或者诽谤他人，侵害他人合法权益的；

8. 危害社会公德或者民族优秀文化传统的；

9. 有法律、行政法规和国家规定禁止的其他内容的。

四、审核流程

1. 对企业自主研发的产品，在研发阶段进行培训；对故事背景、美术素材等进行初步筛查；

2. 自审人员在产品公测前，依据内容审查的相关规定，对产品及其服务内容（包括宣传推广，活动策划）进行审查，对违法违规内容进行记录，并签发初审意见；

3. 对初审有问题的产品，退回研发企业或部门进行修改，并对修改后的内容进行复查；

4. 对内容的合法合规性不能准确判断的，向广东省文化和旅游厅提交申请行政指导；

5. 复查仍有问题的，按照上述 2-4 所规定内容重新进行审核；

6. 在产品公测前，对产品客户端、公司官网、产品官网进行审查，合格后方可公测；

7. 对审查完成的产品，自审人员提出同意进行公测的意见并签字确认，上交内容审查管理工作的主要负责人；

8. 日常对产品和服务内容进行监督检查，包括产品版本更新后的内容、产品客户端、公司官网、产品官网、宣传推广和活动策划等各个方面和环节，发现问题提交检查意见，报本企业内容审查管理工作的主要负责人；

9. 自审人员的所有审查意见应归档留存，保存时间不低于两年。

五、未成年人保护

自审人员需审查网站上的动漫产品不得宣扬淫秽、赌博、暴力或者教唆犯罪等影响未成年人身心健康发展。如动漫产品需满 18 周岁以上的公民阅读浏览的，需添加适龄提示。

六、责任追究

1.对自审人员未能在审查中发现问题的，予以警告处置，多次出现相同这一状况，取消其自审人员资格；

2.对自审人员发现问题，但开发人员拒不修改的，予以警告处置，并通报其上级主管；

3.对自审人员发现问题，但开发人员修改，审查通过后自行予以恢复的，予以严重警告处置，通报其上级主管，并处以罚款若干；

4.对运营人员在运营过程中未通知自审人员，造成不良后果，而自审人员也未及时发现的，予以涉事双方警告处置，责成改正；

5.其他情形造成不良后果的，予以警告处置，并通报其上级主管，保留进一步追责的权力。

七、用户注册

平台采用严格的用户注册流程，设定记录基础密码、身份证登记和用户邮箱等信息，全面保障用户的登记信息完整有效。用户注册成功后，平台将给予每个用户一个用户帐号及相应的密码，该用户帐号和密码由用户负责保管；用户应当对其用户帐号进行的所有活动和事件负法律责任。平台将使用现有的技术，尽力防止用户的个人资料丢失、被盗用或遭篡改。如用户的个人资料丢失、被盗用或遭篡改，平台向用户提供相应的救济途径帮助其找回资料、修复被篡改的资料。

八、跟帖服务

1.按照“后台实名、前台自愿”原则，对注册用户进行真实身份信息认证，不得向未认证真实身份信息的用户提供跟帖评论服务。

2.建立健全用户信息保护制度，收集、使用用户个人信息应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

3.对新闻信息提供跟帖评论服务的，应当建立先审后发制度。

4.提供“弹幕”方式跟帖评论服务的，应当在同一平台和页面同时提供与之对应的静态版信息内容。

5.建立健全跟帖评论审核管理、实时巡查、应急处置等信息安全管理制度，及时发现和处置违法信息，并向广东省文化和旅游厅报告。

6.开发跟帖评论信息安全保护和管理技术，创新跟帖评论管理方式，研发使用反垃圾信息管理系统，提升垃圾信息处置能力；及时发现跟帖评论服务存在的安全缺陷、漏洞等风险，采取补救措施，并向有关主管部门报告。

7.配备与服务规模相适应的审核编辑队伍，提高审核编辑人员专业素养。

8.配合有关主管部门依法开展监督检查工作，提供必要的技术、资料和数据支持。

九、应急响应

1.事件等级：

根据信息安全事件的影响程度等因素将重大信息安全事件分为三个等级：

第三等级：特大信息安全事件，涉及国家安全和社会稳定，造成恶劣影响和严重后果。

第二等级：重大信息安全事件，涉及国家安全和社会稳定，造成较大社会影响和较严重后果。

第一等级：一般信息安全事件，造成一定社会影响的信息安全事件。

2.报告时限：

公司发生以上信息安全事件时，根据等级的不同分别向上级主管部门报告，报告分为口头报告、简要书面报告和专题书面报告：

发生特大信息安全事件时，公司在 2 小时内做出口头报告，24 小时内做出简要书面报告，事件处理结束后 5 日内做出专题书面报告。

发生重大信息安全事件时，公司在 4 小时内做出口头报告，24 小时内做出简要书面报告，相关事件处理结束后 5 日内做出专题书面报告。

发生一般信息安全事件时，公司在 48 小时内做出专题书面报告。

3.处置流程：

由于公司网络环境安全事件（包括火灾、盗窃、破坏、供电等）、网络运行相关事件（包括线路中断、路由障碍、流量异常、域名系统故障等）引发信息安全时，紧急通知我公司负责人，及时消除非法信息，恢复系统，无法迅速消除或恢复系统、影响较大时实施紧急关闭，并及时上报。

一般信息安全事件发生时，向入侵者所在的网络管理员投诉。

重大信息安全事件及特大信息安全事件发生时（如造成重大经济损失，破坏国家信息安全的反动政治言论），及时清除、保留证据，立即向网络和信息安全事件应急小组报告。网络和信息安全事件应急小组接到报告后，立即对发生的事件进行调查核实、保留相关证据，确定事件等级，向上级主管部门上报相关材料。

十、技术安全

在系统运营中，我公司将不定期的对系统的性能进行跟踪，一方面了解系统的工作状态，用于设计系统优化方案；另一方面发现系统运行中存在的各种问题，进行处理及完善，以达到进一步改进系统性能，必要的时候开发补丁软件或进行软件升级，使整套系统的性能发挥到最大。

（一）网站安全保障措施

（1） 网站服务器和其他计算机之间设经公安部认证的防火墙，并与专业网络安全公司合作，做好安全策略，拒绝外来的恶意攻击，保障网站正常运行。

（2） 在网站的服务器及工作站上均安装了正版的防病毒软件，对计算机病毒、有害电子邮件有整套的防范措施，防止有害信息对网站系统的干扰和破坏。

（3） 做好生产日志的留存。网站具有保存 60 天以上的系统运行日志和用户使用日志记录功能，内容包括 IP 地址及使用情况，主页维护者、邮箱使用者和对应的 IP 地址情况等。

（4） 交互式栏目具备有 IP 地址、身份登记和识别确认功能，对没有合法手续和不具备条件的电子公告服务立即关闭。

（5） 网站信息服务系统建立双机热备份机制，一旦主系统遇到故障或受到攻击导致不能正常运行，保证备用系统能及时替换主系统提供服务。

（6） 关闭网站系统中暂不使用的服务功能及相关端口，并及时用补丁修复系统漏洞，定期查杀病毒。

（7） 服务器平时处于锁定状态，并保管好登录密码；后台管理界面设置超级用户名及密码，并绑定 IP，以防他人登入。

（8） 网站提供集中式权限管理，针对不同的应用系统、终端、操作人员，由网站系统管理员设置共享数据库信息的访问权限，并设置相应的密码及口令。不同的操作人员设定不同的用户名，且定期更换，严禁操作人员泄漏自己的口令。对操作人员的权限严格按照岗位职责设定，并由网站系统管理员定期检查操作人员权限。（9）公司机房按照电信机房标准建设，内有必备的独立 UPS 不间断电源、高灵敏度的烟雾探测系统和消防系统，定期进行电力、防火、防潮、防磁和防鼠检查。

（二）用户信息安全

1. 公司平台采用严格的用户注册流程，全面的用户信息登记功能，设定记录基础密码等信息，包括用户私人信息和身份证信息，全面保障用户的登记信息完整有效。公司平台对用户所提供的实名身份信息进行严格的管理及保护，并将使用现有的技术，尽力防止用户的个人资料丢失、被盗用或遭篡改。公司平台未经用户授权不公开、修改、透露用户身份信息资料及其它保密性内容(特殊原因除外）。我司郑重承诺尊重并保护用户的个人隐私，除了在与用户签署的隐私政策和网站服务条款以及其他公布的准则规定的情况下，我司不会随意公布与用户个人身份有关的资料，除非有法律或程序要求。其中，主要内容包括：

1）总经理拥有最高权限，涉及到公司核心用户个人信息的使用时，须由总经理唯一授权。

2）对于用户个人信息，全体员工应当严格遵循保护及保密原则。需指定工作人员方可查询和使用用户个人信息，并记录对用户信息进行操作的人员，时间，地点，事项等信息。未经授权的情况下使用用户个人信息，一经发现，将会被立即辞退。如已违反法律法规的，且已造成重大经济损失的，将会被移交至相关的执法机关依法处理。

2.网络信息安全部在发现用户个人信息发生或者可能发生泄露、毁损、丢失的，应立即暂停为用户提供的服务，并由相关技术工作人员在 20 分钟内进行改密措施。

3.公司对用户个人信息保护情况每年至少自查三次，并记录自查情况，且须及时消除自查中发现的安全隐患。

4.网络用户身份管理制度的落实情况：我司网站已完善好注册登录信息，我司加强对用户的信息的管理，发现法律、法规禁止发布、传输的信息的，应当立即停止传

输，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

5.用户个人用户信息及重要数据境内存储的落实情况：所有查询活动的情况，包括查询人员、查询时间、查询原因等，该数据库都有记录。除用户本人及上级主管监管部门外任何人不得调取用户信息用于他用，建立多重备份制度，对重要资料除在电脑贮存外，还拷贝到光盘及相关移动存储设备上，并由专人负责保管，以防遭病毒破坏而遗失，一经发现严肃处理，情节严重报送公安机关。保证用户的信息私密情况，不会泄露出去，让用户能够放心浏览网站信息。

（三）保密管理制度

1.180 天日志记录

做好访问日志的留存。网站具有保存六月以上的系统运行日志和用户使用日志记录功能,内容包括 IP 地址及使用情况,主页维护者、对应的 IP 地址情况等。建立用户日志留存系统，在数据库日志对应的表为 smslog 表，在用户使用系统时，自动将日志保存到该表中。公司采用了阿里云的数据库备份服务，每天的数据都会在云平台上进行备份，并在本地搭建 nas 系统，用于数据库的本地备份，日志记录的主要内容有：用户上线时间、注销时间、用户活动内容等。系统维护管理部门为安全管理部，定期检测系统功能，具备用户日志数据备份和恢复功能，所有信息都及时做备份。按照国家有关规定，所有用户使用信息和日志保存六个月的原始记录，根据用户需求提供原始数据清单。

2.具有安全审计、有害信息筛查等预警功能

公司采用了腾讯的 tim 的 sdk，借助于腾讯的关键字过滤和舆情监控系统，配合公司的人工审核，防止不法分子传播反动色情敏感信息，保护信息。

3.开设邮件服务的，具有垃圾邮件清理功能

我公司在网站的云服务器及工作站上均安装了相应的防病毒软件，对计算机病毒、有害电子邮件有整套的防范措施和清理垃圾邮件功能。防止有害信息对网站系统的干扰和破坏。防止信息在传输的过程中被非法截获，加固采用 B 级系统解决系统安全问题。加强人员安全培训，制定系统安全技术措施，使用漏洞扫描软件扫描系统漏洞，关闭不必要的端口。采取严格的安全管理措施，加强严格的访问列表、口令加密、对一些漏洞禁止访问。

4.具有实名身份登记和识别确认功能

我公司网站系统具备有 IP 地址、身份登记和识别确认功能,对非法贴子或留言能做到及时删除并进行重要信息向相关部门汇报，设立个人主页服务的，登记个人主页创办者真实身份（姓名、身份证号码、家庭住址）、联系电话等，并能实别身份、上

网 ip 和记录上网时间。同时我公司网站信息服务系统建立多机备份机制,一旦主系统遇到故障或受到攻击导致不能正常运行,可以在最短的时间内替换主系统提供服务。服务器平时处于锁定状态,并保管好登录密码;后台管理界面设置超级用户名及密码,并绑定 IP,以防他人登入。网站提供集中式权限管理,针对不同的应用系统、终端、操作人员,由网站系统管理员设置共享数据库信息的访问权限,并设置相应的密码及口令。不同的操作人员设定不同的用户名,且定期更换,严禁操作人员泄漏自己的口令。对操作人员的权限严格按照岗位职责设定,并由网站系统管理员定期检查操作人员权限 。

（四）其它技术措施

多层防火墙：根据用户的不同需求，采用多层高性能的硬件防火墙对客户托管的主机进行全面的保护。

异构防火墙：同时采用业界最先进成熟的 F5 防火墙硬件防火墙进行保护，不同厂家不同结构的防火墙更进一步保障了用户网络和主机的安全。

防病毒扫描：专业的防病毒扫描软件，杜绝病毒对客户主机的感染。

入侵检测：专业的安全软件，提供基于网络、主机、数据库、应用程序的入侵检测服务，在防火墙的基础上又增加了几道安全措施，确保用户系统的高度安全。

漏洞扫描：定期对用户主机及应用系统进行安全漏洞扫描和分析，排除安全隐患，做到安全防患于未然。

F5bigip 防火墙硬件防火墙运行在 CISCO 交换机上层提供了专门的主机上监视所有网络上流过的数据包，发现能够正确识别攻击在进行的攻击特征。

攻击的识别是实时的，用户可定义报警和一旦攻击被检测到的响应。此处，我们有如下保护措施：

全部事件监控策略：此项策略用于测试目的，监视报告所有安全事件。在现实环境下面，此项策略将严重影响检测服务器的性能。

攻击检测策略：此策略重点防范来自网络上的恶意攻击，适合管理员了解网络上的重要的网络事件。

协议分析：此策略与攻击检测策略不同，将会对网络的会话进行协议分析，适合安全管理员了解网络的使用情况。

网站保护：此策略用于监视网络上对 HTTP 流量的监视，而且只对 HTTP 攻击敏感。适合安全管理员了解和监视网络上的网站访问情况。

Windows 网络保护：此策略重点防护 Windows 网络环境。

会话复制：此项策略提供了复制 Telnet, FTP, SMTP 会话的功能。此功能用于

安全策略的定制。

linux 远程登录采用 1024 位密钥的安全防护，确保服务器万无一失。

DMZ 监控此项策略重点保护在防火墙外的 DMZ 区域的网络活动。这个策略监视网络攻击和典型的互联网协议弱点攻击，例如（HTTP,FTP,SMTP,POP 和 DNS），适合安全管理员监视企业防火墙以外的网络事件。

防火墙内监控：此项策略重点针对穿越防火墙的网络应用的攻击和协议弱点利用，适合防火墙内部安全事件的监视。

总体技术发展策略：

（1）配备专业的维护人员为用户提供服务的系统进行全天候的监控，一旦应用系统发生故障，维护人员可立即解决问题并使系统恢复正常，在要求的时间内正确处理用户的请求服务，对用户的请求进行响应，并回复给用户请求的内容，保证内容准确无误。

（2）用备份技术来提高数据恢复时的完整性。备份工作可以手工完成，也可以自动完成。现有的操作系统都带有比较初级的备份系统。由于备份本身含有秘密信息，备份介质也是偷窃者的目标，因此，计算机系统允许用户的某些特别文件不进行系统备份，而做涉密介质备份。

（3）防病毒。定期检查网络系统是否被感染了计算机病毒，对引导软盘或下载软件和文档应加以安全控制，对外来软盘在使用前应进行病毒诊断。同时注意不断更新病毒诊断软件版本，及时掌握、发现正在流行的计算机病毒动向，并采取相应的有效措施。

（4）补丁程序。及时安装各种安全补丁程序，不给入侵者以可乘之机。

（5）仔细阅读"系统日志"和“用户日志”。对可疑活动一定要仔细分析，如有人在试图访问一些不安全的服务端口，利用 Finger、Tftp 或用 Debug 手段访问用户邮件服务器等。对此系统管理员应加以关注和分析。

（6）信息过滤。系统平台的非法内容过滤子系统对发送的短信内容进行严格的监控，一旦发现敏感、非法、黄色等信息，系统会将此条信息视为无效信息，阻止信息的发送！公司有专人负责过滤内容的收集录入，内容包括中文简体、繁体、英文等各种编码的信息。公司将尽最大限度确保信息的合法性，阻止造成信息安全的非法行为。

十一、主播（作者）管理

1. 作者在平台注册帐户时提供和使用的所有个人信息应当是合法的。前述账号信息在本平台中进行的包括但不限于以下事项：注册本服务帐户、提交相应资质材料、

确认和同意相关协议和规则等事项，均是作者自行或授权他人进行的行为，对作者均有约束力。同时，作者承担以前述账号信息为标识进行的全部行为的法律责任。

2. 若作者发现有他人冒用或盗用帐户及密码、或任何其他未经作者本人合法授权的情形时，应立即以有效方式通知我司（包括但不限于提供作者本人的身份信息和相关身份资料、相关事实情况及您的要求等）。我司收到有效请求并核实身份后，会根据不同情况采取相应措施。若作者提供的信息不完全，导致我司无法核实作者的身份或我司无法判断作者的需求等，而导致我司无法进行及时处理，给作者带来的损失，作者本人应自行承担。
3. 确保网站上的漫画作品拥有著作权或已经著作权人授权，我司有权要求作者提供相关权利证明文件、授权文件、相关机构颁发的权利证书等，作者应当配合。

十二、培训考核

1. 审核人员积极参加文化部组织的企业内容自审人员培训及考核，掌握内容审核的政策法规和相关知识，每月组织员工进行政治学习一次，业务学习二次。
2. 每个部门主管对部门人员进行业务考核，新入职人员通过考核后方可入职，非新员工需每月达到部门所定业绩和任务要求。超标完成任务的，给予奖励；持续半年未完成任务的，以劝退处理。

十三、举报受理

客服部收到用户直接或间接的举报的，必须对用户举报的信息进行记录，了解用户举报内容是否合法合规合理。举报电话：020-38915007

客服部对能够独立判断用户举报内容的，应立即予以解释、解决；不能立即解决的，及时通知负责人协调相关部门主管进行配合，由部门主管及时解决。由客服部对用户纠纷投诉的最终处理结果进行回访登记，记录保存期限 1 年。