字节跳动安全响应中心基本原则与测试规范

第一章 基本原则

1、字节跳动非常重视产品及业务的安全问题，字节跳动安全响应中心（ByteDance Security Response Center）负责收取字节跳动中国区全线产品及应用的漏洞/情报，期待白帽子、安全组织、研究者等能够一起加入，完成“合作式安全报告披露与处置”，为共建良好互联网安全生态而努力。
2、未在收录范围的非中区产品及应用的漏洞/情报，请提交至：security@bytedance.com
3、以漏洞测试为借口，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为的，或以漏洞作为要挟或进行贿赂行为的，我们将不予奖励，并保留进一步追究法律责任的权利。
4、未经授权任何人不得对外披露漏洞/情报细节（包括但不限于在第三方平台上存储、传播或讨论漏洞/情报详情），或利用漏洞非法获利。如您泄露了漏洞/情报信息或利用漏洞/情报非法获利，我们将不给予奖励、已给予的奖励有权收回、封禁平台账号，并对情节严重者保留进一步追究法律责任的权利。若您打算在我们修复漏洞之后公开讨论或向任意第三方披露漏洞，包括但不限于会议演讲，发表技术文章等方式，请提前联系:src@bytedance.com；如需补充漏洞详情或复现录屏，请通过飞书云文档上传视频，禁止使用第三方平台存储漏洞相关信息。
5、字节跳动员工不得参与或通过朋友参与漏洞奖励计划。如经查发现是字节跳动员工参与本奖励规则所述的活动，我们有权不给予奖励，已给予的奖励有权收回，同时封禁平台账号，并将保留进一步内部处理的权利。
6、如果您对漏洞评级结果有争议，欢迎通过漏洞留言板、邮箱:src@bytedance.com 向我们反馈，互相尊重和理性沟通是解决问题的前提，对于捏造事实、恶意诋毁平台或言语攻击、辱骂威胁平台工作人员的行为，我们将不予以奖励，已发放的奖励将追回，同时封禁平台账号，感谢您的理解和配合。
7、您在“字节跳动安全响应中心”平台获得奖励所产生的个税，将由平台统一承担。您应知悉我们为您代扣代缴的个税，属于综合所得的部分，则将体现在个人所得税年度汇算中。
8、当您在“字节跳动安全响应中心”平台进行礼品兑换时，我们将收集您的姓名、通信地址、联系方式、身份证号码等信息。这些信息是我们向您寄送礼品和个税登记扣缴所必须的信息，如果您拒绝提供，我们将无法完成礼品发放。
9、当您在“字节跳动安全响应中心”平台领取现金奖励时，我们还将进一步收集您的的银行卡信息（用于汇款）及身份证号码（用于个税登记和扣缴）。如果您拒绝提供，将无法完成相关款项支付。
10、本评分规则将进行不定期修订，通过“字节跳动安全响应中心”平台发布即生效，发布之后会以醒目方式将新规则供您查阅。

11、如果您对本流程有任何意见建议，邮箱:src@bytedance.com 向我们反馈，您的建议一经采纳，我们将送出精美的礼品作为答谢。

第二章 测试规则

1、禁止进行可能引起业务异常运行的测试，禁止用扫描器或其他自动化工具，只允许手工测试；禁止任何类型的网络拒绝服务（DoS 或 DDoS）测试，或通过软件和工具自动扫描产生大量数据流量的行为。
2、注入漏洞严禁读取表内数据，对于 UPDATE、DELETE、INSERT 等注入类型，不允许使用自动化工具进行测试。（对于可能改变表数据的，需要提前报备。）
3、禁止进行内网渗透测试行为和任何有害化的测试行为，包括但不限于：获取内网权限后在内网使用扫描器、或横向接触非对外开放系统目标、获取内网应用/主机权限/数据、上传 webshell、反弹 shell 等。
4、禁止下载、保存、传播和业务相关的敏感数据，包括但不限于业务服务器以及 Github 等平台泄露的源代码、运营数据、用户资料、登录凭证等，若存在不知情的下载行为，需及时说明和删除；测试过程中获取的相关代码/数据，务必在 SRC 漏洞确认后立即删除，不得非法留存及使用。
5、禁止进行近源攻击或者黑客物理入侵、社会工程学测试或邮件钓鱼等非技术漏洞测试，尤其是禁止使用社工库等非法手段获取用户密码。
6、越权漏洞：越权读取时能够证明读取数量即可，且读取到的真实数据不超过 5 组，严禁进行批量读取；请自备测试账号，敏感操作（增删改）不得涉及线上正常用户的帐号（如需进一步证明危害，请咨询管理员得到同意后进行测试。）
7、 严禁影响线上真实业务和用户数据，或引起客诉事件。包括但不限于向真实用户邮箱、手机、社媒账号等渠道发送测试信息、发起群聊、推送 push 等干扰信息；或通过电话、即时通讯工具等方式直接联系真实用户进行测试。
8、针对业务线专测：专测开始前需和运营报备即将使用的 C2 的 IP 地址，未及时报备将视为未授权攻击行为，会影响最终漏洞奖励；禁止盗用、借用、售卖测试账号，不得擅自修改账号密码、换绑手机号、添加子账号等；禁止利用测试账号对专测范围外的产品和业务测试；测试账号仅限专测时间内使用。
9、禁止使用任何违反平台规定或法律法规的文字、图片、视频作为测试素材。
10、当您在进行重要敏感操作前，请先与管理员报备，得到授权后再进一步测试。
11、关于 AK/SK 泄露相关报告，请直接将 AK/SK 信息提交到平台即可，将由审核验证和确认影响范围及等级，严禁自行深入业务验证危害。
12、根据违规情节严重程度，针对违规人员将采取以下处罚措施：
-取消单个漏洞/情报奖励，已发放的奖励将追回
-封禁账号（您将不能再参加字节的任何奖励计划项目）
-未遵守《网络安全法》，利用安全漏洞进行破坏、损害系统及用户的利益的攻击行为，我们保留追究法律责任的权利。