可接受使用政策（AUP）

RETN
的可接受使用政策对其服务的所有用户都是强制性的。所有客户均受其条款约束，并有责任确保其客户不违反条款。

不可接受的使用可分为四大类：

- - 非法使用
- - 恶意使用
- - 威胁网络完整性的使用
- - 对 RETN 员工的恶意行为

  RETN
  保留随时修改可接受使用政策的权利，以应对新出现的威胁。可接受使用政策的变更自在 https://retn.net/ 上公布之时起生效。

  违反可接受使用政策的后果详见您的管理服务协议。

  禁止：

  非法使用

- - 在提供客户服务的任何地区被视为非法的任何活动；
- - 存储或传输侵犯版权或商标的资料；
- - 存储或传输儿童色情制品；
- -
  使用服务进行或协助进行欺诈、身份盗窃或其他有害或欺诈活动，包括提供或传播欺诈性商品、服务、计划、促销；

-
使用服务传播、控制或以其他方式与恶意计算机程序（病毒、木马、蠕虫、间谍软件和其他恶意软件）交互；

- - 软件或其他媒体盗版；
- - 违反当地进出口法律。

  恶意使用

- 骚扰任何个人或组织，无论是通过公开威胁、威胁性语言，还是仅仅拒绝承认停止和终止要求；
- 对 RETN 网络和 RETN
的任何运营或管理系统进行渗透/漏洞测试，或在未经授权的情况下对其进行访问；

- - 对任何其他实体的网络或系统进行未经授权的渗透/漏洞测试或访问。
- - 以电子方式冒充他人或组织，或采取其他欺骗行为；

- -
  垃圾邮件；未经请求的电子邮件、未经请求的广告、旨在破坏其他服务的信息、含有恶意内容的信息；

- - 电子邮件地址或其他个人在线标识符的植入；
- - 网络钓鱼
- - 未经授权截获信息或其他数据；
- - 运行网络服务，如开放式代理、开放式邮件中继或开放式递归域名服务器。

  威胁网络完整性的使用
  对 RETN 网络或其监控系统的一般干扰。

- - 违反 RETN 供应商可接受使用政策的行为；
- - 导致 RETN 网络成为 DDoS 或其他定向攻击目标的行为；
- - 任何导致我们的 IP 空间被滥用数据库（Spamhaus 等）列入黑名单的行为；
- - 根据政府法令导致 RETN 网络中断的行为；
- - 任何导致其他 RETN 客户服务中断的行为。

针对 RETN 员工的恶意行为

RETN 认真对待员工的保障和福祉，并将始终努力保护他们在安全和温馨的环境中工作的权利。RETN 绝不容忍针对员工的语言或行为，这些语言或行为包括

- 具有侮辱或贬损性质
- 包括任何形式的暴力或人身威胁
- 包括威胁性语言
- 包含与雇员的性别（认为的或其他）、宗教、性别、年龄、种族或任何仇视同性恋的言论有关的任何负面评论