ACCEPTABLE USE POLICY (AUP)

The RETN AUP is mandatory for all users of its services. All customers are to be bound by its terms and in turn are responsible for ensuring their customers do not cause them to breach its terms.

Unacceptable use can be drawn into 3 main categories:
- Illegal Use
- Malicious Use
- Use that threatens network integrity

RETN reserves the right to amend the AUP at any time, to counter emerging threats. Changes to the AUP are enforceable from the moment they are published at https://retn.net/

The consequences for breaching the AUP are detailed within your MSA.

Prohibited Use:

Illegal Use
- Any activity deemed illegal in any of the territories in which the customer service is delivered;
- Storage or transmission of material that is in breach of copyright or trademark;
- Storage or transmission of child pornography;
- Use of the services to carry out, or aid, in fraud, identity theft or other harmful or fraudulent activities including offering or disseminating fraudulent; goods, services, schemes, promotions;
- Using the services to propagate, control or otherwise interact with malicious computer programs (viruses, trojans, worms, spyware and other malware);
- Software or other media piracy;
- Violation of local import/export laws.

Malicious Use
- Harassment of any individual or organisation, whether by overt threat, menacing language, or simply refusal to acknowledge a request to cease and desist;
- Penetration/vulnerability testing of, or unauthorised access to, the RETN network and any of RETN's operational or administrative systems;
- Unauthorised penetration/vulnerability testing of or access to, any other entity's network or systems.
- Electronic impersonation of another individual or organisation or other deceptive practices;
- Spamming; Unsolicited emails, unsolicited advertisements, messages designed to disrupt other services, messages containing malicious content;
- Farming of email addresses or other individual online identifiers;
- Phishing;
- Unauthorised interception of messages or other data;
- Operating network services like open proxies, open mail relays, or open recursive domain name servers.

Use that Threatens Network Integrity
General interference with the RETN network or it's monitoring systems.

- Actions that are in breach of RETN's supplier's AUP;
- Actions that cause the RETN network to become the target of a DDoS or other targeted attack;
- Anything that leads to our IP space being blacklisted by abuse databases (Spamhaus etc);
- Actions which cause the RETN network to be interrupted by Governmental decree;
- Any actions that cause services to other RETN customers to be disrupted.