

Acceptable Use Policy

This Acceptable Use Policy specifies the actions prohibited by Unilynx, to users of the Unilynx Network. Unilynx reserves the right to modify the Policy at any time.

ILLEGAL USE. The Unilynx Network may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

SYSTEM AND NETWORK SECURITY. Violations of system or network security are prohibited, and may result in criminal and civil liability. Unilynx will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following: Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network. Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks. Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

EMAIL. Sending unsolicited mail messages, including, without limitation, Make-Money-Fast (MMF) schemes, chain letters, commercial advertising and informational announcements, is explicitly prohibited. A user shall not use another site's mail server to relay mail without the express permission of the site. As it is against our policy to allow Mail Relaying via Unilynx we implemented a process to prevent this. This means that our Subscribers connecting to SAIX POP may make use of smtp.Unilynx.co.za as their SMTP host but may not use this as a mail relay.

USENET. Posting the same or similar message to one or more newsgroups (excessive cross-posting or multiple-posting, also known as "SPAM") is explicitly prohibited. A seemingly accepted number of simultaneous postings is a maximum of five (5). The posting of Make-Money-Fast (MMF) schemes is explicitly prohibited.

SIMULTANEOUS LOGINS. Username/Password combinations supplied by Unilynx are not transferable. It is the sole responsibility of the end-user to keep his Username/Password confidential. Although we have the mechanism to prevent simultaneous logins violating this agreement constitutes an illegal action.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE POLICY, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A UNILYNX CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THE POLICY BY SUCH CUSTOMER OR END USER.

Unilynx does not in any way support SPAM or any form of NETWORK ABUSE and enforces the Unilynx Terms and Conditions and Acceptable Use Guidelines on a stringent basis when complaints are made. Enforcement of Unilynx Terms and Conditions as well as its Acceptable Use Guidelines for reasons of SPAM or NETWORK ABUSE will result in suspension or termination of account access privileges.

Complaints regarding Illegal Use or System or Network Security issues or e-Mail abuse or USENET abuse or SPAM should be sent to abuse@unilynx.co.za