

Acceptable Use Policy

Version 3.1

3 April 2008

About this policy

1. A "TENET client institution for Internet Services" or "TENET institution" is an institution that has entered into an Agency Agreement with Tertiary Education Network (TENET) in terms of which TENET acts as the agent of the institution for securing Internet connectivity and services to campuses or sites of the institution.
2. "TENET's Internet Services" are the services that are provided to TENET institutions by TENET and/or service providers appointed by TENET in terms of Service Provider Agreements, as provided for in the Agency Agreement.
3. TENET recognizes that many TENET institutions have other business relationships with service providers referred to in Clause 2 above that fall outside the ambit of the Agency Agreement, and recognizes that TENET plays no role in such relationships.
4. This Acceptable Use Policy (AUP) is policy of TENET. It applies to all TENET institutions.
5. Each TENET institution is responsible for ensuring that users of its networks that use TENET's Internet Services comply with this policy. TENET institutions should inform all their users of the contents of this policy and of the obligation to comply with it. TENET may seek to terminate the provision of TENET's Internet Services to any TENET institution that, after having been warned by TENET, continues to violate the provisions of this policy.
6. TENET recommends that each TENET institution should publish and enforce its own Acceptable Use Policy that governs the use of the Institution's campus networks and is consistent with TENET's Acceptable Use Policy.
7. TENET reserves the right to amend this Acceptable Use Policy. Notice of any significant amendments will be given to all TENET institutions and by publication on TENET's web site.

Acceptable Use of TENET's Internet Services

8. Each TENET institution may use TENET's Internet Services for any legal activity that:
 - 8.1 furthers of the aims and objects of the TENET institution;
 - 8.2 complies with the provisions of the Agency Agreement and applicable service provider agreements;
 - 8.3 complies with current good Internet practice as documented in the body of Requests for Comments (RFCs); and
 - 8.4 does not involve any unacceptable use or uses, as defined in Clause 9 below.

Unacceptable Use of TENET's Internet Services

9. The following are unacceptable uses of TENET's Internet Services:
 - 9.1 the transmission, storage or distribution of any material or content where such action would violate any South African or other applicable laws prohibiting child pornography; obscenity; discrimination (including racial, gender or religious slurs) and hate speech; or speech designed to incite violence or hatred, or threats to cause bodily harm.
 - 9.2 the transmission, storage or distribution of any material or content where such action is intended to defame, abuse, stalk, harass or physically threaten any individual in the Republic or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.
 - 9.3 the transmission, storage and distribution of any material or content where such action violates any intellectual property laws including laws concerning local and international copyright, trademarks and trade secrets;
 - 9.4 any effort to use TENET's Internet Services in a way that circumvents or would circumvent the user authentication or security of any host, network or account ("cracking" or "hacking");
 - 9.5 the forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting;
 - 9.6 any attempt to use TENET's Internet Services in a way that breaches or would breach the security of another user's account or that gains or would gain access to any other person's computer, software, or data or otherwise threaten another person's privacy, without the knowledge and consent of such person;
 - 9.7 any activity which threatens to disrupt TENET's Internet Services through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of other networks;
 - 9.8 any activity which in any way threatens the security of the network by knowingly posting, transmitting, linking to or otherwise distributing any information or software which contains a virus; trojan horse; worm, lock, mail bomb, cancelbot or other harmful, destructive or disruptive component.
 - 9.9 any unsolicited mass mailing activity including direct marketing; spam and chain letters for commercial or other purposes, without the prior consent of the recipients of those mails.
 - 9.10 any failure to secure a server that is connected via TENET's Internet Services to the Internet against being abused by third parties as an open relay or open proxy.