

## **ETC Infrastructure Services Usage Policy**

**July 2014**

### **Background**

Infrastructure services - such as computer networks and the Internet, voice systems and radio networks - are essential tools for communicating and sharing information. The ETC is promoting the construction of efficient infrastructure services to provide easy access to information and facilitate the work of the humanitarian community.

While infrastructure services offer great potential benefits, they can also expose organizations to significant risks, due to the uncontrolled nature of the Internet and personal misuse. The risks include dissemination of offensive material or destructive programs, unsolicited e-mail messages with inappropriate content, failure of corporate services or illegal actions in the name of the organization.

It is therefore important to set out policies and guidelines for the efficient use of these services and establish measures to protect organizations from these risks, ensuring that its activities and public image are not damaged.

### **Objectives**

1. This policy applies to the usage of ETC Infrastructure services by the entire ETC user community. The purpose of this policy is to ensure that:
  - Authorized users have access to services and are informed of rules regarding these services, including privacy and security.
  - ETC Infrastructure services are used efficiently and effectively, in the most cost-effective way and in compliance with the rules set out in this policy.
  - Usage of ETC Infrastructure services is compatible with ethical standards of the International Civil Service environment.
  - Disruption of ETC Infrastructure services is minimized.

### **Definition of Terms**

2. *ETC Radio services*: all management, administration and operational facilities that use radios, communication devices and software, and are property of the ETC.
3. *ETC Voice services*: all management, administration and operational facilities that use telephones, communication devices and software, and are property of the ETC.
4. *ETC Data services*: all management, administration and operational facilities that use computers, communication devices and software, and are property of the ETC.

5. *ETC Internet services*: facilities based on the public Internet network that constitute a resource base for the humanitarian community's activities, but are not property of the ETC.
6. *ETC Infrastructure services*: ETC Voice, Data, Internet and Radio services.
7. *Network*: two or more devices (e.g. computers, radios and/or data devices) connected together with the purpose of sharing resources and data.
8. *Internet*: a public and open network connecting thousands of computer networks. Internet utilizes multiple communication protocols to create a worldwide communication medium. It is inherently insecure.

### **Eligibility of Access**

9. ETC provides services to the humanitarian community, consisting of staff from United Nations Agencies, International and National Government Organizations and Stand-by Partners.

### **Use of ETC Infrastructure Services**

10. ETC Infrastructure services are property of the ETC and are used for purposes relating to humanitarian emergency operations. Users are provided with access to these services to assist them in their duties insofar as these duties relate to humanitarian work in emergencies.
11. All users have the responsibility to use ETC Infrastructure services in a professional, lawful and ethical manner.
12. Since technical resources – such as network and storage capacity, radio channels and voice channels – are not unlimited, all users connected to ETC services are responsible for conserving these resources.
13. ETC users must not perform deliberate acts to waste resources or unfairly monopolize resources to the exclusion of others.
14. Based on the environment in which the ETC operates, often without adequate publicly available infrastructure, it recognizes the need for users to access Internet services for personal use (e.g. private email, social networking etc.), provided such use:
  - Where possible is limited to non-working hours
  - Does not interfere with the operation of ETC services
  - Does not violate the rules contained in this policy.

### **Prohibited Use**

15. Anything communicated or done by a staff member in the course of acting for his/her organization or the ETC reflects on the organization's posture, or the image of the humanitarian community. Therefore, to avoid use of services that could result in damage to the humanitarian community, the conditions set out in the following paragraph must be respected.
16. *Material incompatible with the ethical standards of the International Civil Service environment*: ETC Infrastructure services must not be used to disseminate, view or store:
  - Pornographic texts or images
  - Material promoting sexual exploitation or discrimination, racism and violence

- Messages that are derogatory or inflammatory regarding race, age, disability, religion, national origin or sexual preference
  - Information concerning drugs or weapons
  - Destructive codes (e.g. viruses, self-replicating programs) and material concerning 'hacking'
  - Mass mail or chain letters
  - Personal solicitations and promotions
  - Commercial advertisements
  - Any other unauthorized material.
- 17.** ETC Data services may not be used to display, store or send (by e-mail or any other form of electronic communication such as bulletin board, chat room, Usenet group) material that is: fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise inappropriate or illegal.
- 18.** See Annex A for the list of material that ETC considers incompatible with the ethical standards of the International Civil Service environment.
- 19.** Access to Internet is considered illegal or is limited in some countries. Before accessing the Internet, users must first check that local laws will not be violated.
- 20.** In exceptional cases, where there is a legitimate need to use the ETC Data and Internet services to consult material prohibited above (such as for official research on weapons), official written authorization from the head of the involved organization should be presented to the ETC Coordinator.
- 21.** *Copyright law:* users must not copy material protected under copyright law or make such material available to others for copying. Users are responsible for complying with copyright law and licenses that apply to software, files, graphic, documents, messages or other material that can be downloaded or copied. Users must not make copies of or use software unless they know that the copies comply with the license signed between a vendor and his/her organization.
- 22.** Any unauthorized software installed on ETC owned computers will be removed.
- 23.** *The ETC corporate image in public fora:* users must not post ETC-related information to public fora on Internet (such as public discussion or chat groups), unless this refers to ETC materials approved for public publication by the Global ETC Lead Agency.

## **Frivolous Use**

- 24.** Frivolous use of ETC Infrastructure services is discouraged because it wastes resources and/or unfairly monopolizes these resources to the detriment of others.
- 25.** Frivolous use includes, but is not limited to:
- Spending an excessive amount of time on Internet web sites, playing on-line games or engaging in on-line chat groups
  - Downloading games or entertainment software
  - Creation of unnecessary loads by uploading or downloading large files, using file sharing or torrent software or excessive access to streaming audio and/or video files
  - Subscription to real-time automatic information distribution services on Internet, e.g. RSS feeds or newsletters, for information that is not related to official duties

## Internet Access and Security

26. *Connections to Internet:* ETC networks or computers may only be connected to the public Internet through approved access control and/or security systems. Access to and security mechanisms for Internet use are approved and authorized by the ETC Coordinator.
27. *Un-authorized equipment:* to avoid disruption of ETC services, users will not connect networking equipment such as routers or wireless access points to the ETC network without prior authorization from the ETC Coordinator.
28. *User anonymity:* users must not misrepresent, obscure, suppress or replace their own or another user's identity on the Internet or on any ETC information system. The user name, e-mail address, organizational affiliation and related contact information must always reflect the actual originator of a message or posting. The use of anonymous re-mailers or other identity-hiding mechanisms is prohibited; such a practice is not in keeping with the humanitarian community's culture of transparent communication.
29. *Information reliability:* users must be aware that not all information available on Internet may be reliable. While websites of official bodies can be considered authentic and valuable reference sources, there are numerous sites of a personal nature or with suspected credentials that should be treated with caution. The reliability and accuracy of the information contained therein must be confirmed from other sources.
30. It is also relatively easy to fake the identity of another Internet user; as a result, users must not rely on the alleged identity of a correspondent via Internet unless the identity of this person is confirmed through methods acceptable to its own organization.
31. *Sending security parameters:* users should not send any sensitive parameters, such as telephone calling card numbers, passwords or account numbers, through Internet unless the connection has been encrypted.

## Privacy

32. ETC reserves the right to monitor and log any and all aspects of its infrastructure services, including, but not limited to monitoring and logging:
  - The content of ETC owned computers
  - Files downloaded and Internet sites visited.
33. ETC reserves the right to utilize technology that makes it possible to identify and block access to Internet web sites considered inappropriate.
34. The monitoring and logging of staff activities on computer systems, and retrieval of related information are allowed when a legitimate need exists, such as but not limited to:
  - Suspicion of policy violation or illegal activity
  - Maintenance of infrastructure systems
  - Unavailability of a staff member.
35. Monitoring, logging and retrieval are authorized by the ETC Coordinator.

## Responsibilities

### Organizational Responsibilities

36. Heads of organizations are responsible for:
- Implementation of this policy under their delegated authority
  - Ensuring users only request access privileges as needed for their official duties
  - Ensuring users respect the rules described in this policy
  - Reporting cases of non-compliance in their organization to the ETC Coordinator.
37. Definition of traffic policy for ETC Infrastructure services and regulation of service priorities is the direct responsibility of the ETC Coordinator.

### Individual Responsibilities

38. ETC staff and other authorized users who have been granted access to ETC Infrastructure services are expected to abide by the policies and procedures outlined in this document.
39. All users are required to take the necessary precautions to protect the confidentiality of data containing personal or confidential information generated in the performance of their duties. They should utilize any means of protection available to safeguard their activities (e.g. by ensuring that their passwords are secure and changing them when necessary).
40. ETC staff and other authorized users are also responsible for the conduct of any staff they may allow to use network resources through their accounts.

## Policy Violation

41. Violations of this policy should be brought to the attention of the ETC Coordinator.
42. ETC reserves the right to terminate infrastructure services in cases of abuse or misuse of these services.

## Date of Effect

43. This policy takes effect immediately.

## Application of the Policy

44. The policy applies throughout all locations where ETC Infrastructure services are made available.

## References

- Usage of Network Services and Internet, WFP, AD Directive 2003/001
- The International Standard on Information Security; BS ISO/IEC17799 Information Technology — Code of Practice for Information Security

## **Annex A – Material that ETC considers incompatible with the ethical standards of the International Civil Service environment.**

<b>Adult Content</b>	Full or partial nudity of individuals, as well as images of men and women in various stage of undress. Any form of sexual acts. Any form of adult-oriented humor and literature with sexually explicit language.
<b>Drugs</b>	Any materials that pertain to or promote the improper or illegal use of drugs that are regulated, require a prescription, or are illegal. This includes drug-related contraband.
<b>Gambling</b>	Any material that promotes gambling or allows gambling.
<b>Hacking</b>	Any material promoting questionable or illegal use of equipment and/or software to hack passwords, create viruses , gain access to other computers, etc.
<b>Militancy / Extremism</b>	Any material promoting or containing information on militia operations, terrorist activity, war, riots, rebel groups. Advocates of violence to overthrow government.
<b>Racism / Hate</b>	Ethnic impropriety, hate speech, anti-Semitism, racial clubs/conflict.
<b>Violence</b>	Any material promoting or containing information on violent acts, such as murder, rape, violent criminal activity, gangs.
<b>Weapons</b>	Any material promoting, selling, or containing information on guns, knives, missiles, bombs or other weapons.