ACCEPTABLE USE POLICY ON COMPUTING AND NETWORK RESOURCES

The Institute provides computing and network facilities to be used by AIT faculty, staff and students as a community service for the purpose of teaching and research, which includes e-mail usage provided that it has no offensive or abusive character. It is not meant for bandwidth intensive use such as is required for the purpose of entertainment, in particular.

This policy provides guidelines for the appropriate use of computing and network resources provided by the Institute, including academic, residential and remote access (dial-up) facilities. The Institute will take disciplinary and legal measures against any user who has been proven to have abused or blatantly disregarded the Acceptable Use Policy on Computing and Network Resources

1. Acceptable Use Policy

1.1 Access Purposes

1.1.1 The Institute provides computing and network resources only for purposes directly in relation with its mission, i.e. academic and research activities.

1.1.2 Users are not permitted to use computing and network resources for illegal or unlawful activities.

1.1.3 Users are not permitted to use computing and network resources for commercial activities.

1.2 Access Authorization

1.2.1 Users must not access computing and network resources without proper authentication procedure or intentionally enable other to do so.

1.2.2 A user account must be used by its owner only. Users are forbidden to communicate their password or otherwise give access to their account or any AIT computing or network resource to third parties.

1.2.3 Any anomaly discovered in the authentication procedure must be reported to the appropriate authority so that steps can be taken to investigate it and eventually correct it.

1.3 Integrity of computing resources

1.3.1 Users must no attempt to modify or remove computing/network equipment, software or peripherals they do not own without proper authorization.

1.3.2 Users must not :
 * develop, use or disseminate malicious programs, computer viruses and worms,
 * disrupt the activities of other computers or users,
 * access private data or restricted portions of the computing or networking system,
 * damage the software or hardware components of the system.

1.3.3 The computing and network resources are shared by all users and are of finite capacity. Users must therefore avoid capacity and performance degrading usage of the system. Such usage includes but is not limited to:
 * sending of chain-letters or excessive messages, either locally or off-campus,
 * using network protocols using an eccessive amount of bandwidth,
 * printing excess copies of documents,
 * running grossly inefficient programs when efficient alternatives are known by the user to be available,
 * unauthorized modification of system facilities, operating systems, or disk partitions;
 * attempting to crash or tie up computing and networking resources,
 * damaging or vandalizing computing and network facilities, equipment, software or computer data.

1.3.4 Users are allowed to use the computing and network resources only for work purposes. Users should not engage in inappropriate or idle use of the resources nor block their access to other users.

1.4 Privacy issues

1.4.1 Users are forbidden to use other accounts than their own.

1.4.2 Users are forbidden to access files, emails or any form of data not belonging to them.

1.5 Email

1.5.1 Users are forbidden to create and transmit email containing offensive, obscene, indecent, aggressive, menacing, harassing, defamatory, intimidating, unlawful, racist and other unethical messages.

1.5.2 Users are forbidden to send email that does not correctly identify the sender, attempt to hide or disguise the identity of the sender or attempt to hide or disguise the identity of the computer from which it was sent.

1.5.3 Users are forbidden to transmit or forward any email intended to encourage the propagation of copies of itself (e.g. chained letter).

1.5.4 Users are forbidden to flood the mailbox of other users with numerous or large messages with the intention to paralyze their mail system.

1.5.5 Users are forbidden to spread virus or worms or malicious programs.

1.5.6 Users are forbidden to use the email facilities of the Institute for commercial activity

1.6 Mailing List

1.6.1 Users cannot send any email to the Institute's official mailing lists (faculty, staff, students which are moderated by the Institute).

1.6.2 Do not send any private or commercial announcement to any mailing list.

1.6.3 The unofficial mailing lists must only be used to facilitate communications between AIT community members. Every unofficial mailing list must be moderated and no cross posting between them is possible.

1.7 Personal Web use

1.7.1 Publishing personal homepages is allowed only on designated servers.

1.7.2 Personal homepages must not be used for commercial purposes.

1.7.3 Personal homepages must not be used to disseminate offensive, obscene, indecent, aggressive, menacing, defamatory, harassing, intimidating, unlawful, racist, or otherwise unethical information.

1.7.4 Users are forbidden to publish content detrimental to the good name of the Institute on their personal homepages.

1.8 Copyright and software licenses

1.8.1 All software used on any computer must be properly licensed.

1.8.2 Users must not infringe on any intellectual property right while using the Institute's computing and network resources.

2. Operational Policy & Procedure

2.1 Upon request and with authorization by his/her parent academic, administrative or outreach unit in the Institute, a faculty member, a staff or a student will be granted the privilege to use the computing and network resources.

2.2 Every authorized user is given an account, and is allocated associated hardware/software resources

2.3 To defray additional operating cost, outreach units and sponsored projects in the Institute are charged, at approximately cost rate, for the use of computing and network resources

2.4 To the extent possible with its hardware, software and manpower resources, the Institute maintains backup of user files and implements system security safeguards as well as capacity and performance enhancing measures.

2.5 When a user terminates his/her account, the account will be kept active for a period of one month during which the user's files maybe downloaded to another host system.

3. Disciplinary Action

3.1 The following sanctions in case of infringement of the acceptable use policy will be applied, depending on the gravity of the infringement:
* Warning
* Temporary or permanent suspension of account
* Forwarding of the case to AIT administration for further action

Signature : .... Name : ....
Date : .... ID Number : ....