www.nie.edu.sg

1 Nanyang Walk Singapore 637616 Tel: (65) 6790 3888
NTU Reg No. 200604393R

Volume	**Non System Specific Security Policy Volume**
Title	**Computing Acceptable Use Policy**
Date	**Dec 2008**

Review & Approval

Version: 1.2.1

Originator: IT Security

Approval: IT Security Committee

National Institute of Education
1 Nanyang Walk
Singapore 637616

Table of Contents

1 POLICY STATEMENT

1.1 Policy Statement

The security of NIE computing environment is vital as much information and intellectual property is accessed, processed, stored and transmitted across its network and computing facilities. This policy sets forth the institute's expectations of acceptable behaviour on the part of network and computing resources users at the institute by providing standards for appropriate use. These standards of acceptable behaviours also extend beyond the campus community onto the Internet.

1.2 Applicability

This policy applies to all users of the institute's network and computing resources, including staff, trainee teachers and any others granted the use of the institute's network and computing resources. It applies to the use of all network and computing resources owned or contracted by the institute. Network and computing resources refers to wired and wireless networks, computers systems, IP based equipment, peripherals, software and communication infrastructure owned by the institute. Individuals with personally-owned computers, who rely on the institute's network connectivity and/or access the institute's information, are expected to abide by the policies set forth in this document. Personally-owned computers operating in stand-alone mode or networked through a non institute connection are not covered under this policy, but those users are encouraged to consult the usage policies set forth by their Network Service Provider.

1.3 Responsibility

All users of the institute network and computing resources are responsible for complying with the institute acceptable use policy for computing. Misuse of computing resources may result in the loss of access privilege, disciplinary action and/or legal action. Any user who suspects a violation of the institute's computing acceptable use policies, or who has knowledge of potential vulnerabilities or security loopholes in a computer system or network at NIE, should immediately notify Information Security at itsec@nie.edu.sg

1.4 Contact

Questions concerning this policy should be directed to Information Security at email itsec@nie.edu.sg

2 Acceptable Use

2.1 Appropriate Use

Appropriate use of Network and computing resources also refers to usage that does not disrupt or diminish the normal usage of other users. The institute's network and computing resources should be used for official purposes; i.e. to achieve the institute goals of teacher education and research.

2.2 Copyright & Intellectual Property

Users are to respect copyright agreements and intellectual property ownership. Any material that is the work of another, whether explicitly copyrighted or not, should not be distributed or used without appropriate acknowledgement or permission from the creator. The distribution of copyright protected files without the permission of the copyright holder is illegal.

While the institute has been granted permission by software vendors to distribute certain software via the network, it is NOT generally permissible for individual users to distribute the same software to others via the institute network or computing facilities.

2.3 Computer Account

Users are responsible for the use made of their computer accounts. Refer to *Terms & Condition of computer account use*. Users should protect the confidentiality and security of their logon credentials, i.e. user name and password. A strong password should be used and changed regularly. If you suspect that your password has been

compromised, change it immediately and report the incident to Information Security itsec@nie.edu.sg

2.4 Illegal Communications

Users are responsible for the content of their communications. Illegal communications, including threats of violence, obscenity, pornography, and harassment are prohibited.

2.5 Classified Information

Users who maintain classified information, such as staff or trainee teacher records, financial information, the institute's strategic and operational plans are responsible for protecting the confidentiality and integrity of the information. Information should be classified with appropriate classification labels and be revealed on a 'need to know basis' following appropriate approval procedures. Appropriate protection or security controls should be used when transmitting classified information (E.g. Encryption).

2.6 Misuse

The following activities are expressly prohibited at NIE:

a) Using the institute's computer system without proper authorization granted through the Institute or its departments and/or academic groups

b) Using another person's computer account, user name, files, or data without appropriate permission

c) Deleting or tampering with another user's files even if the files are unprotected is improper

d) Masquerading as another account-holder

e) Sharing of computer account and password is explicitly forbidden; users should maintain exclusive control over the use of their password, and protect it from inadvertent disclosure to others

f) Attempting to "crack" or guess other users' passwords or obtaining passwords by other means, such as password capturing programs

g) Attempting to circumvent system security (e.g. breaking into a system or using programs to obtain "root" access)

h) Denying appropriate access to resources to other users (e.g. "ping flooding" another system, sending "mail bombs," or modifying a login file in order to cause a user to not be able to log in)

i) Releasing programs such as viruses, Trojan horses, worms, etc., that disrupt other users, damage software or hardware, disrupt network performance, or replicate themselves for malicious purpose

j) Sending commercial solicitations via electronic mail (i.e. spamming) to individuals or to newsgroups or mailing lists where such advertising is not part of the purpose of the group or list

k) Using mail messages to harass or intimidate another person

l) Reselling of services based on the institute network, such as web hosting, mailing services or the selling of shell accounts

m) Running a proxy server which results in inappropriate or unauthorized access to institute materials to non institute members

n) Advertising commercial businesses or ventures on Web pages hosted by the institute, unless prior authorization has been granted

o) Violations of any laws, such as the distribution of copyright-protected materials (e.g. the distribution of commercial software, music or films in electronic format

without appropriate permissions by the owner, even if the user distributing the materials notifies others of their copyright status)

p) Tampering with, wilful destruction of or theft of any computer equipment, whether it belongs to the institute or to an individual. Tampering includes any deliberate effort to degrade or halt a system, to tie up a system or to compromise the system/network performance. Wilful destruction includes any deliberate disabling or damaging of computer systems, peripheral equipment such as scanners or printers, or other facilities or equipment including the network, and any deliberate destruction or impairment of software or other users' files or data

q) Unauthorized installation of external devices in campus to connect to the institute's networks without prior approval from Computer Services Centre. (E.g. Network storage devices, wireless access points, network switch)

r) Installation of unauthorized software[i].

This list should not be considered to be complete or exhaustive. It should, however, serve as a set of examples of obviously inappropriate behaviours.

[i] Authorised software refers to software purchased by NIE, has a valid license (if it is a limited-use license; has not exceeded the number of copies expressed in the license agreement)