CEIBS IT Policies

Contributed by Administrator
Friday, 20 August 2004
Last Updated Monday, 26 July 2010

Acceptable Usage Policy

1. Introduction

This acceptable usage policy applies to all users of the CEIBS Campus Network and its objective is to ensure that every network user can enjoy a secure and productive working environment.

2. The Network

Network facilities are provided to School members and legitimate users. Users having rights to access network resources do not imply they can transfer the rights to others unless it is explicitly approved by the School. For example, users are not allowed to :

-

Disclose or share the computer account with others.
-

Allow unauthorized users to access the network via his/her own machine.
-

Copy software or data files from network and transfer to others.

Users should be considerate when using the Internet to transmit/receive large files (e.g. multimedia files). Efforts should be made to locate files at local sites and perform at non-office hours. IT Department should be informed prior to download large files.

IT Department is authorized to block some bandwidth consuming services, fox example, streaming media service, at peak of bandwidth utilizing.

Users should not use the network resources for activities that are not related to the school (e.g. commercial and private activities). Downloading by using Peer-to-Peer (P2P) software (such as e-Mule, BT, WebThunder and etc) through campus network is prohibited unless it is explicitly approved by the school. The user whose daily average bandwidth utilization exceeds the benchmark will be subject to penalty defined by the school. The benchmark is adjusted depending on the internet bandwidth and the current benchmark is 400 MB/Day/Client. At first, the client will be blocked to access to any network resources once it exceeds the benchmark. And then one or more of actions listed in Enforcement Section could be taken, depending on the seriousness of the offence.

Network objects (data, program, information) not particularly locked or protected by the system do not imply that they can be altered, deleted or manipulated. This is same as the common understanding that you do not have the right to take away belongings of others although they are not being locked.

4. Security Awareness

Globally speaking, the number of computer and network security incidents has been increasing remarkably in the past few years. Such a worldwide phenomenon is having various impacts on our campus IT infrastructure. User’s security awareness and participation play an important role in maintaining a stable and secure computing environment.

Faculty, Staff and students should become knowledgeable about relevant security requirements and guidelines, and protect all the resources under their control such as access passwords, computers, data and information they acquired.

Computer should have the most recently available and appropriate software security patches, anti-virus software and firewall protection, commensurate with the identified level of acceptable risk.

Adequate identification, authentication and authorization functions should be provided in computer systems and software applications, commensurate with appropriate use and the acceptable level of risk.

Activities outsourced to off-campus entities should comply with the same security requirements as in-house activities.

Resources to be protected include networks, computers, software, data and information. Both physical and logical

integrity of these resources should be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

In any cases, users are advised to consult IT Support Team should you have any queries or problems related to computer and network security. It is sure that a stable and secure IT Environment can be achieved with the efforts from every one of us.

4. The CEIBS Account

Access to restricted resources are provided by means of a CEIBS Account. Users are responsible to maintain a secure password.

In emergency cases, network administrators are authorized to temporarily suspend the access of CEIBS Accounts.

5. Software Copyright and Licenses

China has appropriate copyright and patent laws which govern the use of software and other intellectual properties. The School has also laid down a general policy regarding intellectual properties and software licenses. Users should ensure that all the software (data files inclusive) they install and use does not violate such laws and policies. In particular, users should note the following:

-

All software installed into individual machines must carry valid and appropriate license. This applies not just in offices but also in laboratories and open areas.

-

Users should not copy the software from the campus network and install into other machines without obtaining appropriate licenses.

-

Users should not distribute a software (e.g. setting up ftp server).

6. Email

Email is one of the most important tools for administration and communication in this School. The following are common email problems which should be avoided:

Broadcast mail or Mass mail

Sending inappropriate or irrelevant email to a large group of recipients will not only waste the recipients' time and disk space but can also interfere the normal operation of servers and network. Typical emails considered as inappropriate are:

-

advertisement

-

lost and found

-

announcement of student activities

-

survey and questionnaire

Chain mail

This is equivalent to chain letters, requesting recipient to duplicate a junk mail to others, generating a chain of emails. Users should NOT propagate such mails.

Fake and/or anonymous mail

Email should be sent with the email address assigned by the School. Sending email in the name of others (fake mail) and/or using anonymous mail is considered as acts of dishonesty and could lead to serious disciplinary actions.

Indecent mail

Emails should always be written with proper language and observe common courtesy.

Users should not use bad language or harass the recipient.

7. Pornographic and Indecent Materials

The Laws of China governing the pornographic and indecent materials also apply to files stored in electronic forms. Illegal storage and distribution of such materials is a criminal offense.

8. Enforcement

Depending on the seriousness of the offense, one or more of the following actions could be taken:

- Warning will be given to the user.
- Problematic programs/process will be stopped or be removed from the system.
- Problematic machines will be isolated from network until the problem is rectified.
- User accounts and computer will be suspended from accessing the network for a specified period as determined by Information Centre.