NTC’s ACCEPTABLE USE POLICY FOR ALL SUBSCRIBERS OF NTC DATA NETWORK DEPARTMENT

Policy:

This Policy is a guide to the acceptable use of NTC network facilities and services. Any university, organization or individual connected to NTC's network in order to use it directly, or to connect to any other network(s), must comply with this policy and the stated purposes and Acceptable Use policies of any other network(s) or host(s) used.

Each university or organization is responsible for the activity of its users and for ensuring that its users are familiar with this policy. In addition, each university is encouraged to maintain and enforce its own Acceptable Use policies. The provisions of this policy govern all use of the Services, including any unsupervised anonymous network access offered by universities or organizations.

The following guidelines will be applied to determine whether or not a particular use of the Services is appropriate:

- Users must respect the privacy of others. Users shall not intentionally seek information on, or represent themselves as, another user unless explicitly authorized to do so by that user. Nor shall Users obtain copies of, or modify files, other data, or passwords belonging to others.

- Users must respect the legal protection applied to programs, data, photographs, music, written documents and other material as provided by copyright, trademark, patent, licensure and other proprietary rights mechanisms.

- Users must respect the integrity of other public or private computing and network systems. Users shall not intentionally develop or use programs that harass other users or infiltrate any other computer, computing system or network and/or damage or alter the software components or file systems of a computer, computing system or network.

- User should be consistent with guiding ethical statements and accepted community standards. Use of the Services for malicious, fraudulent, or misrepresentative purposes is not acceptable.

- The Services may not be used in ways that violate applicable laws or regulations of government of Pakistan.
- The Services may not be used in a manner that precludes or significantly hampers network access by others. Nor may the Services be used in a manner that significantly impairs access to other networks connected to NTC's network.
- Connections which create routing patterns that are inconsistent with the effective and shared use of the Services may not be established.
- Unsolicited advertising/spam (intentionally generated) is not acceptable. Advertising is permitted on some Web pages, mailing lists, news groups and similar environments if advertising is explicitly allowed in that environment.
- Repeated, unsolicited and/or unwanted communication/spam of an intrusive/hacking nature is strictly prohibited. Continuing to send e-mail messages or other communications to an individual or organization after being asked to stop is not acceptable.

The intent of this policy is to identify certain types of uses that are not appropriate, but this policy does not necessarily enumerate all possible inappropriate uses. Using the guidelines given above, NTC may at any time make a determination that a particular use is not appropriate.

NTC will not monitor or judge the content of information transmitted via the Services, but will investigate complaints of possible inappropriate use. In the course of investigating complaints, NTC staff will safeguard the privacy of all parties and will themselves follow the guidelines given in this policy and in NTC's Privacy Policy. NTC will only release sensitive, confidential or personally identifiable information to third parties when required by law, or when in NTC's judgment, release is required to prevent serious injury or harm that could result from violation of this policy.

Remedial Action

- When NTC learns of possible inappropriate use, NTC staff will notify the university or organization responsible, who must take immediate remedial action and inform NTC of its action.

- NTC will assist the university or organization in identifying the nature and source of the inappropriate use and in implementing remedial action if requested. Provided the university or organization implements remedial action promptly, NTC will take no further action.

- If NTC is unable to contact the university or organization, or if the university or organization is unable to implement remedial action, NTC reserves the right to pursue remedial action independently. Wherever possible, NTC will pursue remedial action with the least impact to the overall service for the university or organization.

- Should the situation be considered an emergency, and NTC deems it necessary to prevent further inappropriate activity, NTC may temporarily disconnect a university or organization from NTC's network.

- If temporary disconnection is deemed necessary by NTC staff, every effort will be made to inform the university or organization prior to disconnection, and every effort will be made to re-establish the connection as soon as it is mutually deemed safe.

Definitions

Network: In information Technology, a network is a series of points or nodes interconnected by communication paths. Network can interconnect with other networks and contain sub networks.

Integrity: Integrity, in terms of data and network security, is the assurance that information can only be accessed or modified by those authorized to do so. Measures taken to ensure integrity included controlling the physical environment or networked terminals and servers, restricting access to data, and maintaining rigorous authentication practices. Data Integrity can also be threatened by environment hazards, such as heat, dust and electrical surges.

Spam: Unsolicited means that the recipient has not granted verifiable permissions for the message to be sent.

Hacking: The word "hacking" is often used, for what we call a "compromise" is an attempt that breaks into systems to damage it, or for the purpose of getting illegitimate access to resources.

Emergency: An emergency is defined as: "Serious security incidents that require immediate attention to prevent harm to an individual, to protect information from loss or damage that would be difficult or impossible to correct or to deal with serious on-going denial of service attacks."

Subscriber: Any department or NTC or any other organization, universities, DSL/Dialup Clients or any entity using the IP connectivity of NTC Data Network Department is a Subscriber.