IT and Network Usage Policy of
International Islamic University, Islamabad

POLICY STATEMENT

Users of International Islamic University network and computer resources have a responsibility to properly/fairly use and protect those information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information technologies.

POLICY PURPOSE

The purpose of the IT and Network Usage Policy is to help ensure an information infrastructure that supports the basic missions of the University in teaching, learning and research. Computers & IIUI network resources are the property of the University & are powerful enabling technologies for accessing and distributing the information and knowledge developed at the University and else where. As such, these are strategic technologies for the current and future needs of the University. Because these technologies leverage each individual's stability to access and copy information from remote sources, the users must be mindful of the rights of others to the privacy, intellectual property and other rights. This Usage Policy codifies what is considered appropriate usage of IT facilities and services with respect to the rights of others. With the privilege to use the information resources of the University comes a specific responsibility outlined in this Policy.

SUMMARY

Users of University information resources must respect copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other information resource of users. This policy covers the appropriate use of all information resources including all IT facilities/services and the information contained there in.

APPLICABILITY

This policy is applicable to all University students, employees and to others (e.g. guests) permitted to use International Islamic University resources. This policy refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University. This includes networking devices, personal digital assistants, IP-telephones, wireless devices, personal computers, workstations ,minicomputers, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

POLICIES

Copyrights and Licenses:

Computer users must respect copyrights and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

Integrity of Information Resources:

Computer users must respect the integrity of computer-based information resources.

i. Modification or Removal of Equipment

Computer users must not attempt to modify or remove computer equipment, software, or peripherals as these are the property of the University.

ii. Encroaching on Others' Access and Use Computer

Users must not encroach on other's access and use of the University's computers, networks, or other information resources, including digital information. This includes but is not limited to attempting to access or modify personal, individual or any other University information or other resources for which the user is not authorized; sending chain-letters, unsolicited bulk electronic mail either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the users; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer, network or other information resources; or otherwise damaging or vandalizing University computing facilities, equipment, software, computer files or other information resources.

iii. Unauthorized or Destructive Programs

Computer users must not intentionally develop or use programs which disrupt other computer or network users or which access private or restricted information or portions of a System and / or damage software or hardware components of a system. Computer users must ensure that they don't use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than permitted in network guidelines. The use of any unauthorized or destructive program may result in legal action for damages or other punitive action by any injured party, including the University.

iv. Academic Pursuits

The University recognizes the value of research and development, computer security, and the investigation of self-replicating code (e.g., computer viruses and worms). The University may restrict such activities in order to protect University and individual computing environments, but in doing so will take account of legitimate academic pursuits.

Unauthorized Access

Computer users must refrain from seeking to gain unauthorized access to information resources/services or enabling unauthorized access.

i. Abuse of Computing Privileges

Users of University information resources must not access computers, software, data or information, or networks without proper authorization, or intentionally enable others to do so, regardless s of whether the computer, software, data, information, or network in question is owned by the University. For example, abuse of the networks to which the University belongs or the computers at other sites connected to those networks will be treated as an abuse of University computing privileges.

ii. Reporting Problems

Any defects discovered in the system as well as in the network must be reported to the appropriate system administrator deputed in local IT Support Office, so that steps can be taken to investigate and resolve the problem. The problem can be reported on the telephone, via official email or in writing, at the respective blocks IT Support Offices.

iii. Password Protection

A computer user who has been authorized to use a password may be subject to disciplinary action if the user discloses the password or otherwise makes the account available to others without permission of the system administrator. For protecting sensitive data, it is always advisable to use strong passwords & avoid common or easily guessable names.

Usage of IT Facilities

Computer users must respect the rights of other computer users. Most University systems provide mechanisms for the protection of private information from accessing by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of University policy. Only authorized system administrators may access computer users' files with permission of actual owner for maintenance purposes. System administrators will report suspected unlawful or improper activities to authorities.

i. **Prohibited Use:** Use of the University's computers, network or electronic communication facilities/services (such as electronic mail, instant messaging, or any other systems with similar functions) to send, view or download fraudulent, harassing, obscene, threatening, or other material that are in violation of University policy is prohibited.

ii. **Mailing Lists:** Users must respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin-boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the lists' purpose. Persons

sending any materials to a mailing list, which are not consistent with the list's purpose, will be taken as having sent unsolicited material.

iii. **University Official Email:** University official email signifies the authority and legalizes an email subject and purpose. Care will be taken at all levels to use official emails when corresponding with University officials, students and staff. The same holds true in connection with any directive received or forwarded for action to any department. Commercial or private email addresses will not be entertained for any official correspondence. Care will be exercised to curtail wasteful printing and replaced with official emails as far as possible.

The University provides email and other IT facilities to all its employees and students. Any employee/student can avail email facility by simply filling a form "E-mail Signup Form" available on official website. IIUI reserves the right to suspend/delete any account allocated but the data and password of email is strictly confidential. Even the email administrator has no option to view the data/password of individual email accounts.

To facilitate email users the following email groups were also created:

Group 1: Includes all Deans, Directors General, Directors and Chairpersons.

Group 2: Includes all Faculty members

Group 3: Includes Officers and Staff members

Group 4: Includes all Students

Group 5: Includes all ASA members

Group 6: Includes all IIU email account holders

Note: Any new Email Group can be created with the approval of DG/VP (AF&P).

The purpose of all above e-mail groups is to facilitate the group members to internally communicate events and official notifications collectively.

a) Email allocated by IIUI will be strictly used for official/professional communication only.

b) A group member can send email to his/her relevant email-group only.

c) The emails should not contain any ads, complaints, unrest, vulgar, racist, sexist or hatred material. Any email containing any of these will not be circulated to groups and strict action may be taken against the senders.

d) If a person needs to report/complain something, he/she needs to send that through proper channel to the IIU authorities rather than circulating to the whole groups.

e) Generation of emails to a large list directly is also strictly prohibited and comes under spamming, which may lead to account suspension by service provider. If something needs to be circulated, it should be sent to the desired group with a copy of official notification attached.

f) Any email-user found violating the above mentioned policies will be reported to IIU authorities for necessary action.

g) The Moderator of a group will be appointed from the relevant department. For example Academics Section will have its own moderator for the "Students" group. The Moderator will be responsible to screen out the emails sent to its relevant email group.

h) Official correspondence must not be made through private email accounts instead the official IIU email account must be used.

i) The official email account will also be closed in following cases:

   i. After retirement or termination of services of an employee. The copy of the relevant notifications from HRD will be sent to Webmaster.

   ii. After completion or termination of the degree program of a student. The copy of the relevant notifications from Academic Department will be sent to Webmaster.

   iii. A warning notification will be circulated to both official and alternate email addresses before finally closing the email account to provide the chance to shift the personal data from official email account within 3 to 6 months.

j) Social networks and online newspapers should not be accessed through IIU Intranet during office hours. All such sites will be blocked on the IIU Intranet. Similar measures will be taken to control the Internet usage in IIU Hostel premises to provide more Internet bandwidth for serious researchers by stopping online streaming, gaming, etc.

k) New groups will be created to facilitate communication between officers in 17 and above and for employees in scale below 17.

iv. Printing: Shared printing in every department will be utilized and logs of printing activities will be submitted to departmental heads before demanding new toners or new printers. System Administrators will ensure print sharing and maintenance of print logs at every department. The Duplex Printing option should be used to save paper stationery.

v. Domain: Any computer owned by IIUI will always form the part of central domains maintained in the University and all such computers will be serviced and maintained by the IT department. Any personal computer not forming part of the centralized domains will not be serviced by the IT department.

vi. Advertisements: In general, the University's electronic communication facilities/ services should not be used to transmit any personal commercial advertisements, solicitations or promotions.

Information Belonging to Others

Users must not intentionally seek or provide information, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of the actual owners.

Privacy

Users connected to the network must not try to violate the privacy of the other users in the network. System administrators will report suspected unlawful or improper activities to the proper authorities.

i. **Political Use:** University information resources will not be used for partisan political/religious/ labour-welfare activities.

ii. **Personal Use:** University information resources should not be used for personal activities not related to appropriate University functions.

iii. **Commercial Use:** University information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies of the University or with the written approval of a University authorities having the authority to give such approval. Any such commercial use should be related to University activities.

SYSTEM ADMINISTRATOR RESPONSIBILITIES

The system administrators have responsibilities to the University as a whole for the system(s) under his/her jurisdiction & should use reasonable efforts:

i. To take precautions against theft or for damage to the system components.

ii. To faithfully execute all hardware and software licensing agreements applicable to the system.

iii. To treat information about, and information stored by the system's users in an appropriate manner and to take precautions to protect the security of a system or network and the information contained there in.

iv. To promulgate information about specific policies and procedures that governs use of the system and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.

v. To cooperate with the system administrators of other computer systems or networks, whether within or outside the University, to find and correct problems caused on another system by the use of the system under his/her control.

vi. To ensure any computer owned by the IIUI, will always form part of the central domains maintained in the University and all such computers will be serviced and maintained by the IT department. Any personal computer not forming part of the centralized domains will not be serviced by the IT department.

Policy Enforcement

Where violations of this policy come to his or her attention, the system administrator is authorized to take reasonable actions to implement and enforce the usage and service

policies of the system and to provide for security of the system as per permission provided by the competent authority.

Suspension of Privileges

A system administrator may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of the computer system or network, after taking permission from IT authorities.

Security of IT Equipment at Hostels

The security of the IT equipment installed at Hostels, is the responsibility of the Hostel Administration and the Security Guard on duty. The IT Center will only provide technical support according to the complaints, the keys of the cabinets will be kept by the hostel administration and whenever required any maintenance job, the IT Center will take it and return back after completion of the job. Proper log of usage of these keys will be maintained in a register placed in Hostel's Admin Offices.

Internet Services in the University

The Internet and related services in the University will be provided centrally from Network Operation Center (NOC) to all the offices/academic blocks of the University. The following will be must to cope with security demands of the Government Agencies:

a. All computer systems in the University premises must be part of the centralized Network Domain.

b. A unique username/password will be issued to each student, and employee.

c. The Internet service will be only accessible from the computers joined on Domain, and without Domain credentials, the Internet services will not be provided.

The IT Staff

The IT manpower working in different Faculties, Administration, Institutes will work under the administrative control of IT Center. The IT Center periodically has to rotate the IT support staff from one Institute/Faculty/Office to another according to their performance and to get knowledge of the services at different departments. The IT Center Staff matters like, leaves, ACRs, Promotions will be written by the IT Center.