Sindh Madressatul Islam University, Karachi

INFORMATION TECHNOLOGY POLICY

1. INTRODUCTION

1.1 Overview

IT Administration Unit’s intentions for publishing IT Usage Policy are not to impose restrictions that are contrary to SMIU’s established culture of openness, trust and integrity. IT Administration Unit is committed to protecting SMIU's students, faculty, staff and the University from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP are the property of SMIU. These systems are to be used for academic and research purposes in serving the interests of the University, and of our employees and students in the course of normal operations.

Effective security is a team effort involving the participation and support of every SMIU employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

1.2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at SMIU. These rules are in place to protect student, faculty, staff and SMIU. Inappropriate use exposes SMIU to risks including virus attacks, compromise of network systems and services, and legal issues.

1.3 Scope

This policy applies to faculty, employees, students, consultants, temporaries, and other workers at SMIU, including all personnel affiliated with third parties. This policy applies to all equipment that are owned or leased by SMIU.

2. GENERAL GUIDELINES

2.1 IT Equipment and Data Ownership

1. While SMIU's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Campus Systems remains the property of SMIU. Because of the need to protect SMIU's network, management cannot guarantee the confidentiality of personal information stored on any network device belonging to SMIU.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. IT Administration Unit recommends that any information that users consider sensitive or vulnerable be encrypted.

4. For security and networks maintenance purposes, authorized individuals within SMIU may monitor equipment, systems and network traffic at any time, per IT Administration Unit’s Audit Policy.

5. SMIU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.2 Security and Proprietary Information

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by University confidentiality guidelines.

1. Any loss or theft of IT equipment must be immediately reported to the higher authorities.

2. For sensitive office data, specifications, student data, and research data, employees should take all necessary steps to prevent unauthorized access to this information.

3. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.

4. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by

logging-off (control-alt-delete for Windows XP /Windows 7 users) when the host will be unattended.

5. It is responsibility of respective user to make sure that his/her computer is safe from un-authorized access. It is sole responsibility of user to safeguard PC data from virus, unauthorized access and loss.

6. Postings by employees from a SMIU email address to SMIU Blogs, Social Media and newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SMIU, unless posting is in the course of business duties.

7. All hosts used by the employee that are connected to the SMIU Internet/Intranet/Extranet, whether owned by the employee or SMIU, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

9. Password is a unique key of an individual user to access SMIU computing resources. It is vital to choose a password that is hard for others to guess and guard it carefully. It is preferable to use a password of minimum 8 characters that include both alphabets and numbers. Users must change their computer\Email login password frequently and should hide and write passwords in secure places.

10. Default password expiry duration is 60 days so password will be expired after this duration. Expiry alert starts generating warnings 10 days before expiration. It is recommended to change the password before expiration to ensure security and confidentiality.

11. For security purposes a user is allowed only five chances to properly login to the network. If wrong password is supplied five times a user’s account is disabled. If the account is disabled the user may contact Network Administrator to enable the account.

12. If a user forgets his/her password, he/she should contact the Network Administrator for password reset. A user cannot ask System Administrator to reset password of any other user. The network administrator may ask any proof for the ownership of the account.

13. Users are not allowed to Login on any other user’s computer without their permission.

14. Users must protect their computers and the SMIU network from computer viruses. All computer users must ensure that antivirus software is installed on their computer

and that virus protection is enabled. No user should disable virus protection nor must antivirus software be prevented from scanning system files.

15. All media, email, and internet downloads must be scanned for viruses.
16. IT Center has configured every computer on the network to get automatic updates of antivirus software. Every user must make sure that this facility is available on their computer for the protection of their machine.

17. Users must report any suspicion of virus attacks immediately to IT center.

18. It is the responsibility of each computer user to protect all sensitive information of SMIU. Users must refrain from unnecessary sharing of files and folders as this may put sensitive data at risk.

19. Users may not test or implement any products known to compromise the confidentiality, availability or integrity of SMIU resources, data and information. It is illegal to possess, distribute, use or reproduce programs for scanning networks (such as tools used as packet sniffers, hacking, key logger etc).

20. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential.

21. Examples of confidential information include but are not limited to: examinations material (e.g. question papers, award list, etc.) university private, corporate strategies, competitor sensitive, trade secrets, specifications, lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

22. Postings by employees from a SMIU email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SMIU, unless posting is in the course of business duties.

23. All hosts used by the employee that are connected to the SMIU Internet/Intranet/Extranet, whether owned by the employee or SMIU, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.

2.3 Unauthorized Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting services).

Under no circumstances is an employee/student/staff of SMIU authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing SMIU-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the unacceptable use.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SMIU.

2. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, malware, spams, e-mail bombs, etc.).

4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5. Using a SMIU computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

6. Making fraudulent offers of products, items, or services originating from any SMIU account.

7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

2.4 System and Network Activities

1. Port scanning or security scanning is expressly prohibited unless prior notification to IT Center is made.

2. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

3. Circumventing user authentication or security of any host, network or account.

4. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

5. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

6. Providing information about, or lists of, SMIU employees to outside SMIU unless directed by SMIU own policies.

2.5 E-mail and Communication Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, VOIP or messaging, whether through language, frequency, or size of messages.

3. It is mandatory for all employees to use SMIU domain e-mail for official correspondence.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within SMIU's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SMIU or connected via SMIU's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet, newsgroups (newsgroup spam).

8. Using someone else’s telephone line without permission for dialing out any number.

9. Individuals who are provided access to University computer facilities and to the campus-wide communications network assume responsibility for their appropriate

use. The University expects individuals to be careful, honest, responsible, and civil in the use of the University network and computers. Computer and network facilities are provided primarily for their educational use and doing official duties. These facilities have tangible value. Consequently, attempts to circumvent accounting systems or to use the computer accounts of others will be treated as forms of attempted theft.

10. Individuals may not attempt to damage or to degrade the performance of SMIU's computers and network and should not disrupt the work of other users.
11. Individuals may not attempt to circumvent security systems or to exploit or probe for security holes in any SMIU network or system, nor may individuals attempt any such activity against other systems accessed through SMIU's facilities.
12. Individuals assume personal responsibility for the use of their accounts.
13. Physical theft, rearrangement, or damage to any University computer or network equipment, facilities or property is strictly prohibited, and disciplinary action may be taken. This includes all public computer labs, network equipment, wiring and links.
14. Users with personal computers on the SMIU network are expected to take reasonable precautions to ensure the security of their systems. All computers require a valid up to date virus-scanning program. Individuals may be held responsible for misuse by others that occur on their systems.
15. Users are not permitted to register external domain names that reference systems on the SMIU network. It is prohibited to use SMIU's network for commercial purposes. It is prohibited to connect any secondary physical network to the LU network without authorization.
16. Providing services or running applications that consume excessive bandwidth on the SMIU network is prohibited.
17. No SMIU system is to be used for any illegal or criminal purpose. Users must observe intellectual property rights including, in particular, copyright laws as they apply to software and electronic forms of information.

18. File Sharing Software is prohibited on the SMIU University Network**.**

19. File Sharing software including those listed below (but not limited to), are prohibited on the SMIU network (including residence halls, apartments, classrooms, public spaces and faculty/staff offices.

Aimster	Gnutella	Madster
Ares (All versions)	Hotline	Monolito
BearShare	Imesh	Napster
Bitorrent	Kazaa (All versions	Neo Napster
Bulbster	LimeWire	WinMX

20. Because our network and Internet connections are shared by many university services (the University Library, SMIU University website, Electronic Mail, etc.),

we monitor this traffic constantly to ensure reliable service for everyone. File sharing software can account for a large portion of traffic on our network.

21. Streaming media (such as streaming news clips, streaming audio programs, etc.) are permitted as they use significantly less bandwidth. However, during peak hours, any bandwidth-intensive application may be terminated to ensure continued services to the rest of the university.
22. If you have file sharing applications on your computer, you must remove them. Simply disabling these applications may not mitigate their affect on our network as these applications share your computer with the entire Internet in the background, generating an enormous amount of traffic. If you have any questions, please contact the Information Technology Administration Unit.

3. COMPUTER AND NETWORK USAGE POLICY

IT policy is necessary for following reasons.

- To pave the way for paperless communication.
- Provide physical security for computers and IT equipments
- Maximize availability of computers and network resources.
- To secure computers and IT equipment from un-authorized access, hacking and Virus attacks by using centralized security policy
- Confidentiality of Information
- Efficient and Appropriate Use

SMIU Computer and Network Usage Policy apply to:

- Intranet/Internet/Email Usage
- Users/Group Email Accounts request
- Web Publishing/Posting on news groups/forums
- Computer Hardware
- Computer Software
- IT Support Procedure

3.1 Intranet/Internet/E-mail usage

The use of the SMIU Intranet/Internet/Extranet provides benefits to all SMIU users. Intranet/Internet/Extranet, however, are shared facilities and must be used properly. Choking of bandwidth by a single user can impact the work of hundreds of other users who are using the same, shared facility. Internet and email should not be used to access or disseminate illegal, defamatory, or potentially offensive information/content. Computer and network usage will be governed by the following policy:

1. Users should not exceed their allotted quota for saving data in centralized Folders.
2. Personal and Departments Centralized Storage folders are for official data only. No personal material should be stored in this area.
3. Playing Online Videos, Songs, and Games etc is strictly prohibited. Violations can lead to strict disciplinary action.
4. Internet usage must be for educational, teaching, research and official purposes only.
5. Only one machine should be connected to one Data Point, unless allowed by Information Technology Administration Unit and higher authorities. Sharing an IP/MAC address or setting up of proxy servers for multiple users is strictly prohibited unless authorized by IT Manager.
6. Peer to Peer file sharing / Download software like Kazza, Get right, Morphous, download accelerator, Flash get, etc must not be downloaded.
7. Avoid sending and receiving *.Zip files. If receiving Zip file is necessary then scan it with installed antivirus before opening it.
8. Email should be checked and downloaded frequently. Unused accounts will be disabled.

9. All official communication should be done by using official SMIU email.
10. SMIU Email should be used for official purposes only. No objectionable material should be disseminated using SMIU network/email resources.
11. All SMIU computer users must respect the copyrights in the works that are accessible through SMIU network. No copyrighted work may be copied, published, disseminated, displayed, performed, or played without permission of the copyright holder except in accordance with the fair use or licensed agreement.
12. The university authorities may charge users for the Internet/Intranet/Extranet/e-mail usage to cover the expenses incurred on ITAU. Income generated by such charges would go to the ITAU head only. No other section/department is authorized to charge/collect money for the Internet/Intranet/Extranet/e-mail usage.
13. ITUA may require identity of machines (e.g. MAC address) to allow or block access of machine to the Intranet. In case of violations of IT policy, or improper use of Intranet, ITUA may block any machine at any time without any prior notice.

3.2 User/Group E-Mail Account

1. Any user/group that has account in SMIU domain will also have SMIU E-mail account. All employees are required to send their official e-mails through the officially assigned SMIU e-mail id.
2. All users will be able to access their e-mails from SMIU Intranet as well as from remote site.
3. A user/group will be assigned only one email account. Every project/program executed by SMIU will be allotted a public email address, which will be used for correspondence related to that project.
4. User Email accounts are private and confidential and strictly for use by the individual for whom they are created and the individuals will be held responsible for any improper or unethical use of their account.
5. Any new appointment will request for account in SMIU domain through proper channel. The request is addressed to IT Manager. The required group permissions and access rights be mentioned in the written request.
6. Users will get user id and password from respective department chairman.
7. The default storage quota for email is 150 MB for teachers & officers and 50 MB for students. However, this quota can be increased in special circumstances with the approval of IT Manager.
8. Teachers, students and Administration officer’s accounts will be in their department’s organizational unit (OU) under the SMIU domain. These accounts can be officially used for intra and interdepartmental e-communication. All users are required to check their accounts for any possible mails regularly.
9. In case of a group account (e.g. a class, research group, etc.), the request for account be forwarded by the class teacher, or by group leader through departmental/sectional head.

3.3 Password Policy

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

1. Never write passwords down.
2. Never send a password through email.
3. Never include a password in a non-encrypted stored document.
4. Never tell anyone your password.
5. Never reveal your password over the telephone.
6. Never hint at the format of your password.
7. Never reveal or hint at your password on a form on the internet.
8. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
9. Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
10. Report any suspicion of your password being broken to your IT Administration Unit.
11. If anyone asks for your password, refer them to your IT Administration Unit.
12. Don't use common acronyms as part of your password.
13. Don't use common words or reverse spelling of words in part of your password.
14. Don't use names of people or places as part of your password.
15. Don't use part of your login name in your password.
16. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
17. Be careful about letting someone see you type your password.
18. Minimum Length - 8 characters recommended
19. Maximum Length - 14 characters
20. Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
    1. Lowercase
    2. Uppercase
    3. Numbers
    4. Special characters such as !@#$%^&*(){}[]
21. Passwords are case sensitive and the user name or login ID is not case sensitive.
22. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 10.
23. Maximum password age - 60 days
24. Minimum password age - 2 days
25. Account will be locked after 4 failed login attempts.
26. Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal of additional help desk calls. Therefore

depending on the situation, the account lockout should be between 30 minutes and 2 hours.

27. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. they can press the CTRL-ALT-DEL keys and select "Lock Computer".
28. Rules that apply to passwords apply to passphrases which are used for public/private key authentication
29. The password under no circumstances, be communicated to any other person. The user must change the initial/default password before starting to use the account and protect this password.

3.4 Web Publishing/Job Postings/News

1. The uploading of information on the SMIU website would be through IT Manager. The IT Manager will instruct the webmaster or web developer to upload the desired content.
2. Information of all Exams and results of SMIU must be published on the website. It will be sole responsibility of respective departments for the correctness of Data.
3. All SMIU advertisements sent for publishing in the newspaper must also be sent to the Webmaster for web publishing.
4. Information about research journals will be sent to webmaster for publishing.
5. All the material to be uploaded to the SMIU website must be emailed to the web Master addressed to IT Manager at least 48 hours before it is to be posted on the website.
6. All website update requests will be served on first-come-first-serve basis. Under special circumstances task priorities may be changed. Such a change will require an approval of Manager IT.
7. The decision to post any unofficial item on news would be decided by the Manager IT or by any other ITAU employee nominated by the Manager IT.

3.4 ITAU Support Procedure

IT Administration Unit is responsible for overall functioning of IT infrastructure at SMIU which includes SMIU Network, Servers, Switches, Routers, Cabling, Access Points, Desktops, Laptops, and Printers, etc. ITAU takes steps for servicing, maintaining and upgrading of these entities.

IT administration unit operates a Helpdesk to resolve daily operating issues of users. User can contact ITAU through phone, email or Web portal (Web Portal will be made in due course of time).

Local PBX Number: 336

Email: admin@smiu.edu.pk, support@smiu.edu.pk

3.5 Security and Use of e-resources

The assets that must be protected include:

1. Computer and Peripheral Equipment.
2. Communications Equipment.
3. Computing and Communications Premises.
4. Video Conferencing / VOIP
5. System Computer Programs and Documentation.
6. Information.

4. IT EQUIPMENT

4.1 IT Equipment Ownership

IT by no means is the owner of any asset. All IT equipment are owned by respective departments. IT only provides Technical Support, guideline and help to all users for taking maximum benefits from these resources. Therefore IT cannot assign assets on its own.

4.2 IT Equipment Request

Any person/Department requesting any asset must get it approved from appropriate authorities on the IT ASSET REQUEST FORM (IARF). Approved form must be submitted to the IT Department.

Subject to availability of equipment, installation will be made within five working days/one week. If the equipment is not available it will go through the acquisition phase. It may then take longer for providing the equipment.

INFORMATION TECHNOLOGY ADMINISTRATION UNIT

EQUIPMENT REQUEST FORM

Date: -------------------

Name: --

Designation and scale: --

Department: ---

Location: -------------------------------------- Telephone: --------------------------------------

Required Equipment: ---

Justification: --

-------------------------------- ---

User Name and Signature Department Head Name and Signature

Vice Chancellor

Note: Form must be approved by Worthy Vice Chancellor before submitting to IT.

For IT Use:

Equipment installation Date: …………………….

Equipment Description: …………………………...

Model……………………..……………………

S#: ……………………………………………

-------------------------- ----------------------

Hardware Custodian Received By User

IT Manager

INFORMATION TECHNOLOGY ADMINISTRATION UNIT

LOGIN / EMAIL ACCOUNT CREATION FORM

Date: -----------------------

First Name: ------------------- Middle Name: ------------------- Last Name: -----------------

Department and Class: --

Employee / Enrollment#: --

----------------------------- User Name and Signature and Signature

------------------------------ Department Head Name

For IT Use:

Email ID created date: ---

Email ID……………………

Note: Password will be directly communicated to user.

------------------- IT Representative

---------------------- User

Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment/admission. Legal action (if their action found to be illegal), and criminal liability (if their action is found to be criminal).

Definitions

Term	**Definition**
SMIU	Sindh Madressatul Islam University.
Employee	The entire people who are being employed by Sindh Madressatul Islam University, Karachi, including officers, teaching & non-Teaching.
Students	All the students that are enrolled in University in any discipline and in any department, including Bachelors, Masters, Post-Graduate, M-Phil, and PhD.
Spam	Unauthorized and/or unsolicited electronic mass mailings.
OU	Organizational Unit of the Sindh Madressatul Islam University Domain.
E-mail	Official SMIU domain based e-mail **username@smiu.edu.pk**

Approval

Proposed IT policy Guidelines for Sindh Madressatul Islam University, Karachi (To be approved by statutory bodies)