Somaiya Vidyavihar

Information Technology Services: IT General Policy

1. Purpose of Policy

1.1. The SVV is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative, and service functions.

1.2. Users of the Information Technology facilities must comply with these requirements which have been designed to allow all users to make optimal and legitimate use of the facilities. The SVV requires users to accept the IT policies.

2. Definitions

2.1. SVV: Somaiya Vidyavihar

2.2. ITS: Information Technology Services at SVV

3. Application & Scope

3.1. This policy applies to all usage of the IT Facilities. The policy covers computing, collaboration and communications facilities.

3.2. All users should be aware of the policy, their responsibilities and legal obligations. All users are required to comply with the policy.

4. Policy Principles or Objectives

4.1. The SVV IT Facilities are provided to assist staff, students and other authorized users to conduct bona fide academic and administrative pursuits.

4.2. All users must accept full responsibility for using the SVV's IT Facilities in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people. Use must be in accordance with SVV's policies.

4.3. All system administrators and users understand their own responsibilities for protecting the IT network.

4.4. An effective availability of network operates at all times, and that rapid tracking down and resolution of any network problems by the Information Technology department (IT) is facilitated.

4.5. Interruptions to the service and unnecessary calls on support staff are minimized.

4.6. The following general principles apply to usage of IT Facilities:

- An authorized user of the SVV IT Facilities has an assigned user account, which is identified by a SVVNetID.
- A user may be given access to a range of IT Facilities and is to use these facilities in a manner which is ethical, lawful, effective and efficient. A user may only use those facilities they have been authorized to use.

K. J. SOMAIYA COLLEGE OF ARTS & COMMERCE VIDYA-VIHAR MUMBAI-77

I/C Principal
K. J. Somaiya College of Arts & Commerce
Vidyavihar, Mumbai - 77

- The above does not apply where a user provides access to their account to an authorized support person.
- The SVV discourages the storing of passwords due to the security risks this poses.
- Each user, while using their account, is responsible for:
  - all activities which originate from their account;
  - all information sent from, intentionally requested, solicited or viewed from their account;
  - publicly accessible information placed on a computer using their account.
- No user shall:
  - attempt to subvert or damage the security of any of the SVV's IT facilities.
  - attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software or data.
  - attempt to interfere with the operation of any of the SVV's IT Facilities.
  - attempt to subvert or damage any restriction or accounting control of any of the SVV's IT Facilities.
  - attempt unauthorised access to any SVV's IT Facilities.
  - The above may not apply to authorised support staff in the performance of their duties.
- The SVV network and IT Facilities, including email and web servers and other similar resources, may not be used for:
  - the creation or transmission (other than for properly supervised and lawful teaching or research purposes) of any material or data which could reasonably be deemed abusive, offensive, obscene or indecent;
  - the creation or transmission of material which the average person deems likely to harass, intimidate, harm or distress;
  - the creation or transmission of defamatory material;
  - the transmission of material that infringes the copyright of another person;
  - the unauthorised transmission of material which is labelled confidential or commercial in confidence;
  - unauthorised commercial activities or unauthorised personal gain;
- No user shall use the SVVIT Facilities for private gain or for financial gain to a third party.
- All users must use somaiya.edu email id for any official communications.
- Report any evidence of violation of these rules to the appropriate authorities.

K. J. SOMAIYA COLLEGE OF ARTS & COMMERCE
VIDYA-VIHAR MUMBAI-77

5. Network

5.1. The SVV operates a computer network, which is designed to facilitate communication within the campus for students ,staff, and other authorised users in support of teaching, research, administrative and service functions.

5.2. You must take reasonable steps to ensure that your use of the SVV network or services does not cause an excessive amount of traffic on SVV internal network or its external network links. IT may, pending investigation, disable computers or user accounts which appear to cause unreasonable consumption of network resources.

6. File Storage

6.1. Do not gain access or attempt to gain access to any files owned by someone else unless the owner has specifically granted access or a 3rd party data access request has been granted.

6.2. Anti-virus products must be used at all times. You must not introduce malicious code, including viruses, network worms, Trojan, spyware or any other form of malware.

6.3. Do not download or install software / attach hardware to the network which may compromise the security of our data, the network or other users.

7. Software and Software Licences

7.1. ITS will not install any software on SVV's hardware where the correct licences have not been purchased or there is an insufficient number of correct licences in place.

7.2. The installation of demo or evaluation software will only be actioned where its use complies with the licence i.e. evaluation software should be used to evaluate if the product should be purchased and not used in place of a licensed copy.

7.3. Users are responsible for making use of software and electronic materials in accordance with software licensing agreements.

7.4. No trial software to be used in any of the SVV's hardware.

8. Computer Laboratories

8.1. A user of a computer laboratory shall abide by any instruction or signage as provided by authorised personnel and shall provide relevant identification on request.

8.2. This policy apply without exception;however the SVV reserves the right to apply additional policy and rules specific to individual laboratories.

8.3. All computer laboratories should be manned (laboratory incharge / faculty) till the time the laboratory~~time laboratory~~ is kept open.

8.4. Laboratory Incharge is responsible for all the equipment and maintenance.

9. Equipment

9.1. Extra care should be taken to ensure that laptops and portable equipment (e.g. pen drives) are kept securely. Concerned users are responsible for data held on items of portable equipment.

9.2. Upon leaving employment with the SVV concerned users should return laptops and/or portable equipment to HR or HOD.

9.3. Old or unused laptops or portable equipment should be returned by concerned users to the ITS.

9.4. The returned equipment shall be reused, recycled or disposed of depending upon its age and usability.

9.5. Laptops issued to the staff and faculty should be connected to the campus network once every week. This is required so that the windows and antivirus updates are updated in the system periodically.

10. Administration and Implementation

10.1. SVV treats misuse of its IT Facilities seriously. Violations of the conditions of use of IT Facilities may result in temporary or indefinite withdrawal of access, disciplinary action may be taken.

10.2. A user's access will be withdrawn in response to a written request from an appropriate staff member . Access may also be withdrawn by ITS in response to a suspected policy violation.

10.3. Users are encouraged to report any misuse and any reports will be treated as confidential.

11. Security

11.1. All computers used within the SVV that are owned by the SVV require the current version of our Anti-Virus software to be installed. If a user suspects that their computer does not have the software installed they should immediately contact the local system administrator.

11.2. If connecting a personally owned device to the SVV's Wi-Fi system, it is the responsibility of each individual user to ensure that they have the latest anti-virus software installed on their device.

11.3. Users must not interfere with the operation of the Anti-Virus software installed on University-owned devices, or change its configuration, unless the Designated Authority has granted permission.

11.4. Users must scan all portable media (USB sticks, memory cards, etc.) for viruses prior to use.

11.5. If you receive any suspicious electronic communication or suspect your machine is infected by malware please contact the local system administrator for assistance.

12. Password Policy

Users should at all times comply with the following guidelines:

- Authorised users are allocated a Login (a single username and a single password, or several pairs as required), and must ensure that nobody else uses it. The user is responsible for the security and confidentiality of the username and password.
- Users must not use anyone else's username/password.
- Users must not obtain or try to obtain anyone else's password.
- Users are explicitly prohibited from divulging their passwords to third parties. Users must not allow anyone else to use their account even with their supervision. Users may be held responsible for the actions of, and any consequences of, any other individual using their account. Users must inform local system administrator immediately if they suspect someone else of using their user id/password.
- Passwords must never be written down, printed or stored on-line.
- Passwords should be changed at least once in a year.
- When you change your password it should not be the same as any of your previous two passwords.
- Passwords must be at least seven characters in length, or the maximum allowed by that system if less than seven.
- Passwords must contain three of the following types of characters, uppercase alphabetical, lowercase alphabetical, numerical, or symbols.
- Passwords must not be obvious to third parties, i.e. using your name, username, or words such as 'password' are not acceptable.
- Office computers must not be left unattended when logged in unless a password protected screen-lock is used (Windows key + L).
- The use of password protected screen lock is recommended to all users.
- Shared computers must not be left unattended when logged in.

13. Monitoring

The SVV has the right to monitor any aspect of its computer systems that are made available to you. The following monitoring measures are in place:

- Software installation and usage is monitored as part of the SVV ongoing software audit.
- Additionally, SVV would like to draw everyone's attention to the fact that CCTV is in operation for the protection of employees ,students and assets.

14. Network Security

The network permits high speed connections to the Internet and is at present operated with a minimum of restrictions to enable flexibility of communications between connected computers. This flexibility of operation, however, poses potential security risks. In order to safeguard the stability, integrity and security of the SVV's IT network, steps need to be taken by IT and each department to ensure that machines under their control are properly managed to minimise the risks.

15. Computer and Network Administration Policy

The following general policy statement applies to all computers in the SVV :

1. All computers, computer peripherals, telephone and mobile phone equipment, software and software licenses procured by SVV and that are used at SVV are the property of SVV and do not belong to individual members of staff or students
2. Every device connected to the SVV wired network must be subject to formal system administration
3. Responsibility for administration and security of computers is held by the institute level administrator.
4. Access to any network connected computer must be via a logon process that identifies and authenticates the user.
5. Accounts used by system administrators and end users should be disabled immediately after leaving the institute or retirement.
6. Computers in open areas should be physically secured.
7. Personal equipment may not be connected to the wired SVV network except with specific permission from IT.

16. Responsibilities of Local System Administrators

Institute level Systems Administrators (or Network Administrators) are responsible for the secure operation of computers. The responsibilities of System Administrators include:

16.1. Installation and maintenance of the operating system and network connection in order to reduce the chance of unauthorised access.

16.2. Ensuring that systems security patches are kept up to date where possible and such that the service is not adversely affected.

16.3. Putting in place systems monitoring in order to detect breaches in security, and alerting Network staff in the event of any breach.

16.4. Ensuring that all software is properly licensed.

16.5. Putting in place adequate backup procedures.

16.6. Installing adequate virus protection software.

16.7. Ensuring that all network shares are secure.

16.8. Disconnecting a system, individual workstation or software if necessary to protect or maintain service.

17. Legal

17.1. Users are personally responsible for the content of their emails and their contributions to discussion boards, synchronous chat or similar forums and shall indemnify SVV against any liability incurred by SVV, which arises out of any such communication or contribution.

17.2. Each user of SVV's Systems undertakes that he or she will not hold the SVV liable for any material contributed to a discussion board or synchronous chat by another person, which is defamatory of that SVV's user.

"In case of any concern / issue feel free to notify us on hr@somaiya.edu or techsupport@somaiya.edu with subject line as "Policy for Employee Category"

Dr.Preeti Rawat
Director & Head HR
Editor-In-Chief Business Perspectives and Research (BPR)
(Sage Publications,Scopus, ABS,ABDC and UGC Care list II)

Mahaveer Devannavar
General Manager – Information Technology

K. J. SOMAIYA COLLEGE OF ARTS & COMMERCE VIDYA-VIHAR MUMBAI-77

I/C Principal
Somaiya College of Arts & Commerce
Vidyavihar, Mumbai - 77