# ICT POLICY FOR SAURASHTRA UNIVERSITY

## A. GENERAL GUIDELINES APPLICABLE TO ALL USERS

1. Users shall be responsible for protecting any information used and/or stored online their systems and accounts.

2. Users shall report any weaknesses found in information security, any incidents of misuse or violation of this policy to the proper authorities.

3. Users shall not attempt to access any data or programs on systems maintained by department for which they do not have authorization or consent of the custodian of the data/programs.

4. Users shall not make copies of copyrighted software except as permitted by law or by the owner of the copyright.

S. Users shall not purposely engage in the activity with the intent to:
i. Harass other users; degrade the performance of the systems;
ii. Deprive an authorized Department user access to a Department resource;
iii. Obtain extra resource beyond those allocated;
iv. Circumvent security measures, or gain access to system for which authorization has not been given.

6. Electronics & Communication facilities (voice or data) are for authorized use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on Office systems.

7. Only authorized users shall download, install or run security programs or utilities that reveal weaknesses in the security of a system (for ex. Vulnerability scanners, password crackers, etc).

8. All users are responsible for adhering to the standards outline in this security policy document when using UNIVERSITY computing facilities.

9. Any employees found to have violated this policy shall be subject to disciplinary action as per the discipline and conduct rules of University.

## B. GUIDELINES FOR SECURITY OF DESKTOP/HARDWARE

1. All computers shall be registered.
2. All computers shall be located away from environmental hazards.
3. All computers shall be clearly marked with the name of the owner/group responsible for system.
4. All offices shall be locked. Office keys shall be registered and monitored to ensure they are returned when the owner leaves the Office.

5. All desktops in public areas shall be secured. Equipment located in publicly accessible areas or rooms that cannot be locked shall be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.

6. Hard disks shall be secured. External hard disks shall be secured against access, tampering or removal.

7. Critical data backup media shall be secured on fireproof vaults or in another building.

8. Password facilities shall be utilized to ensure that only authorized users can access the system. Where the Desktop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures. Two-factor authentication shall be considered to access the systems. Automatic screen locking facilities shall be used whenever the system is kept idle.

9. Password policy of the organization must be implemented for desktop access, user authentication and authorization.

C. DATA AND SOFTWARE AVAILABILITY
1. Only authorized software shall be used.
2. All related service packs and patches shall be applied.
3. Any extra software more than the required shall not be installed
4. A Logbook shall be maintained, which shows the installed software.
5. Data and software Integrity shall be checked at regular periods.

D. CONFIDENTIAL INFORMATION
1. Sensitive and confidential information shall be encrypted, where appropriate.

2. Printers used to produce sensitive and confidential information shall be monitored ..

3. Disk shares shall not be used, where sensitive and confidential information is stored.

4. File shredders shall be used to delete sensitive files on desktops.

5. SSL/SSH communication shall be used, whenever sensitive and confidential information is accessed on network.

E. SOFTWARE
Software is protected by copyright law. Unauthorized copying/use of software is a violation of Copyright Act. Anyone who uses software shall understand and comply with the license requirements of the software. The organization is subject to random license audits by software vendors.

F. VIRUSES (MALWARE)

1. Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and :shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software shall be made as soon as a problem is found.

2. To decrease the risk of viruses and limit their spread.

3. Install authorized antivirus software

4. System shall be configured with auto update. On stand-alone systems, manual signature update shall be considered.

5. All software shall be checked before installing them.

6. The system shall be immediately isolated if found to be contaminated.

G. GUIDELINES RELATING TO PASSWORD AND ITS CONSTRUCTION

1. Users must be responsible for all activities performed with their personal user IDs and must not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

2. All user- level passwords (e.g., email, web, desktop computer, etc.) shall be changed at least once every three months.

3. All access codes including user 10 passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

4. Passwords of personal accounts should not be revealed to the boss or any co-worker even while on vacation.

5. Passwords shall not be revealed on questionnaires or security forms.

6. The same password shall not be used for each of the systems to which a user has been granted access e.g a separate password to be used for an NT account and a UNIX account should be selected.

7. The same password shall not be used for official accounts and nonofficial personal accounts e.g. an e-mail accounton .holtmail.com .

8. The "Remember Password" feature of appliccltions (e.g., Eudora, OutLook, Netscape Messenger) shall not be used.

9. Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

10. All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.

11 . If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

12. The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

13. First time login should force changing of password.

**Guidelines for Constructing a Password:**

All user-level and system-level passwords must conform to the following general guidelines described below.

a. The password shall contain more than eight characters.
b. The password shall not be a word found in a dictionary (English or foreign) .
c. The password shall not be a derivative of the user ID.
d. The password shall not be a slang, dialect, jargon etc.
e. The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.
f. The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.
g. The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
h. The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321 , etc. or any of the above spelled backwards.
I. The password shall not be any of the above preceded or followed by a digit (e.g. , secret1 , 1 secret).
J. The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as weJl and other characters (e.g., !@# $%'&·(L +1--=I·{}O:";'<>?,.n.
k. Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

**Suggestions for choosing passwords:**

Passwords may be chosen such that they are difficult-to-guess *yet* easy-to remember.

Methods such as the following may be employed:

a. String together several words to form a pass-phrase as a password.
b. Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.
c. Combine punctuation and/or numbers with a regular word.
d. Create acronyms from words in a song, a poem, or any other known sequence of words.
e. Bump characters in a word a certain number of letters up or down the alphabet.

f. Shift a word up, down, left or right one row on the keyboard.

All individual users having accounts for accessing systems/services in the Department domain, and system administrators of Department servers/ network equipments shall ensure the implementation of this policy. Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.

**GUIDELINES FOR USAGE OF PORTABLE MEDIA**

**THREATS:**

USB portable storage devices pose two kinds of threats:

1. They allow users to bypass perimeter defenses, including firewalls and email server anti-malware, and potentially introduce malware into the office. Since the malware enters the network from an internal device, it may go undetected until significant damage is caused to the network.

2. Portable storage devices allow employees, social engineers, and intruders in general to remove sensitive information from an organization's premises. This information might include protected classified information. The impact of an information compromise by either of these threats, including the accidental loss of information through the loss of a device, could be devastating. An organization's reputation might be damaged beyond repair.

**ADMISSIBILITY:**

The same rules that are applicable in the office to mobile phones are applied for any memory device with external connectivity like Pen drive, digital camera, digital watches, PDA, Palmtops.

**USERS:**

1. The officers are responsible for the safe custody of devices and contents stored in the devices issued to them.

2. Each eligible officer, on a need base will be issued two USB memory devices.One shall be used for storing classified data and it should not be shared. Theother device may be used for exchanging non-clc!ssified documents.

3. The classified data normally is encrypted befor.e copying into the USB device designated to store classified information. The key to decrypt files should not exist on the same device where encryption data exists.

4. For Top Secret information separate USB pen drives should be used as per Guidelines.

5. Unused data on USB devices shall be wiped using multiple pass process (like wipe/eraser software).

6. The officers should not allow to mount the pen drives belongs to outsiders on Intranet systems.

7. The officer should scan the portable device, which was used on any outside system including the PC at home for any virus iJefore copying any data on the official system.

8. If the USB Pen drives are taken outside office fClr official purpose, the classified documents should not be copied on to any system, which does not belong to the office. If the documents are to be modified, the pen drive should be mounted on system, which is not connected to network. Thf~ modification of documents of pen drive should be carried out without copying into the target system.

9. The officer should return the USB devices issued to him upon transfer or retirement.

10. In case of damage or malfunction of device, the! same shall be returned to the concerned official for issue of a substitute.

11. If the USB device is not a functional requiremen~ after issuance, the same shall be returned.

**VISITORS:**

1. Visitors are not allowed to carry any portable media without permission. If it is necessary to allow the visitor to use USB memory device for any reason, it should be used only on designated systems meant for presentation purpose in the office. Under no circumstances the pen drive:s belong to visitors be mounted on systems belong to the office.

2. The pen drive should be removed from the system immediately after copying the file(s) into the designated systems.

3. It should be ensured that nothing gets copied from those systems designated for presentations to USB memory device belongs to visitor.

**IT STAFF:**

1. A record shall be maintained for procurement, issue, return, movement, destruction of the portable devices.

2. A unique serial number shall be assigned to eac.h device and clearly marked on it. Different serial number sequence should bl3 used for pen drive used for general data and pen driver for classified data.

3. The office wilt issue two types of USB pen-drive devices, which are easily distinguishable in shape, color and make. Officers will be given instructions, which one of the two will be used for classified data.

4. The USB memory device used for storing dassified data should have a password protect mechanism for read, write, delete.

5. All obsolete USB devices shall be physically destroyed after returning to store.

S. A verification of USB devices should be carried out by store in-charge at regular intervals of three months by way of self certification by officers that the pen drives issued to them are under their safe custody.

7. On systems connected on intranet, DepartmE!nt witt provide access control software for the device after implementation o'f Active Directory, so that only authorized users will copy data to USB Pen drive.

8. Use of portable devices should be disabled in the BIOS setting of workstations and BIOS should be password protected on those workstations, which are not required to use portable devices.

9. Portable devices of the visitors should be checked before entry for the malicious software and prior to departure for any classified information.

**I. GUIDELINES FOR INTERNET, E-MAIL, INSTANT MESSAGES AND PEER-TOPEER FILE SHARING**

1. Users should keep their email and internet credentials secure
2. Users should be aware that electronic mail is vulnerable to unauthorized access and modification by third parties.
3. User should not use the Internet or email, Resources for any kind of personal or non-University purposes or purposes incidental to them. "University Purpose ~ herein should refer to valid university purpose that can be used to improve the products and services provided by University.
4. All users should use UNIVERSITY assigned email addresses for official communication
5. Users should not forward work sensitive emails originating from either UNIVERSITY or Customer domains to any free public email domains.
6. Users should not use their personal email addresses as contact addresses for conducting UNIVERSITY official operations.
7. Users should not use their email and internet services for any unauthorized purposes targeting UNIVERSITY colleagues and other general public for areas, such as but not limited to:
a. Use of the Resources in connection with surveys, contests, chain letters, junk e-mail, spamming, or any duplicative or unsolicited messages
b. Defame abuse, harass, stalk, threaten or IJtherwise violate the legal and privacy rights
c. Publish, distribute, or disseminate any inappropriate, profane, defamatory, Infringing, obscene, indecent or unlawful material
d. Transmit, upload or download any material that potentially contains viruses, Trojan horses, worms, time bombs, or any other harmful or deleterious programs
e. Forward or send messages that have radal or sexual slur, political or religious solicitations, or any other messagEl that are in-appropriate and/or has the potential to cause UNIVERSITY, harm or embarrassment.
f.Access of pornographic sites, special interest giroup, web sites, internet trading and personal web browsing.
8. Users should not indulge in unlawful activities souch as accessing unauthorized Resources, hacking, introducing any computer contaminant or computer virus,

committing acts, which may disrupt use of the Iresources, or aiding or abetting any of the above. The users should neither USE! UNIVERSITY resources to such as BUT NOT LIMITED to scanning UNIVERSITY computer systems/devices nor scanning/launching attacks on the computer systems/devices of other organizational networks.
9. Users should acknowledge their misuse of the resources may result in the violation of intellectual property rights of third parties. Users should ensure that all proprietary material acquired by them through use of the resources, have been obtained through valid licenses from the suppliers or proprietors.
10. Users should acknowledge that their misuse of the resources may result in the breach of confidentiality with relation to UNIVERSITY or third parties, and they should adhere to all confidentiality and restriction of publicity obligation they are bound by within UNIVERSITY and to third parties.
11. Violations of these terms governing the use of the resources with or without intention wilJ result in restriction of access to the resources and may include action which requires an investigation and appropriate disciplinary action to be taken, up to and including termination from services.
12. Internal emails should be used for electronic approvals and valid documentary evidence.
13. Users are not permitted to set up any type of proxy servers on the network, other than for approved requirements. All internet traffic must be routed through UNIVERSITY pproved proxy services only.
14. At any time and without prior notice, UNIVERSITY management reserves the right to examine personal file directories and all other information stored or transmit inclusive of email on computers connected to UNIVERSITY.
15. Customer deliverables exchanged over internet through file transfer should be on an encrypted channel.
16. User contact database information and related personal records should be adequately protected.
17. Connection times should be restricted to Applications such as internet access.
18. Other office communication systems such as EPABX (Private Telephone exchanges), fax systems, audio and video conferencing facilities and distribution of mails should be dequately protected.
19. Legal Department advice should be taken while implementing Cryptographic Controls.
20. Encryption controls should be implemented as required on business critical applications accessible over internet.
21. Emails from university domain exchanged with internet domains should be subject to necessary Antispam and Antivirus checks, with suitable technology controls.
22. Users should not involve in misuse of email facility in any ways which could bring in undesirable impact to the employees/organizationlThird Parties/General Public.
23. Users should also be cautious of the information received in their UNIVERSITY email addresses especially if auto-forward to customer supplied email addresses is enabled.
24. Users should not involve in initiating or propagating chain emails which are not relevant to work.
25. The users should use UNIVERSITY provided Internet facilities and should not access Internet by connecting a modem or any other such devices.

**J. GUIDELINES FOR PREVENTING CREATION/SPREAD OF MALICIOUS CODE**

1. Department employees and other users of UNIVERSITY are not permitted to use Department resources to install, run, copy, store, distribute or develop any form of malicious software code intended to obtain, destroy, secretly install or modify information/data stored, run or used on any computer system.
2. Department employees and other users of UNIVERSITY are not permitted to use Department resources to run or manipulate software applications or programs to perform a malicious function which can obtain, destroy, secretty install or modify information/data stored, run or used on any computer system.
3. System Users are responsible for adhering to this policy.
4. Authorized personnel working in Cyber Security group, Forensics are permitted to use any programs/code for the specific purpose.
5. Any employee found to have violated this policy should be subject to disciplinary action as per the rules of the organization.

**K. GUIDELINES FOR USAGE OF ANTI-VIRUS SOFTWARE**

This guideline applies to all Windows / Linux and other O.S. based servers and workstations and mail servers operating on UNIVERSITY:
1. All windows / Linux and other O.S based servers and workstations shall install anti virus software with auto-update feature enabled for signature updates.
2. Anti-virus scan should run at least once a week. In sensitive Departments, the scan shall be carried out everyday.
3. All mail servers shall check for virus on all incoming and outgoing mail.
4. Anti-virus server log should be maintained for a period of six months.

**L. GUIDELINES FOR TAKING BACK UP**

1. Responsibility of taking backups for individual's Desktops/Laptops should rest with respective user.
2. Information Owner in conjunction with System Administrator should identify the critical server resources that need to be backed up.
3. Appropriate backup media should be chosen by information owner based on the criticality data and retention period.
4. Periodicity of backup (backup schedule) should be determined by Information owner and backups of critical server resources should be taken by System Administrator as per the schedule,

**COMPUTER NETWORK**

Networked computers require more stringent security than stand-alone computers because they are access points to computer networks. While UNIVERSITY operators have responsibility for setting up and maintaining appropriate security procedures on the etwork, each individual is responsible for operating their own computer with ethical regard for thers in the shared environment.

The following considerations and procedures must be emphasized in a network environment:

1. All files downloaded from the Internet shall be checked. Downloading shareware files shall be avoided .
2. Mail usage policy of the organization shall be strictly adhered .
3. Downloading of any type of files from unknown sources shall be avoided.
4. Care shall be taken while pressing 'OK' on POPUP menus. They may implant spy ware or key loggers on your system.
5. All scripts to run automatically shall be disabled.
6. Internet browsers shall be configured for not to running java scripts.
7. All software shall be tested before installation to make sure it doesn't contain a virus/ worm that could have serious consequences for other personal computers and servers on networks.
8. IP Filters shall be enabled wherever possible.
9. Regular BACK-UP important files shall be taken.

**HODs/Officers LAN Level Security Guidelines:**

This level of security will be applicable to various Government HODs/Officers Local Area Network (LAN) within UNIVERSITY. The Top level authority for the respective HODs/Offices will be responsible for any violation from the defined guidelines from this level.

1. HODs/Offices LAN Guidelines would include following :
2. N/W Access Control
3. System Accounts Management
4. User Verification Process
5. Operating System, Application, Database configuration
6. Asset Management
7. Back Up
8. Blogging

**I. DEPARTMENTAL NETWORK LEVEL SECURITY GUIDELINES:**

This level of security will be applicable to Academic Departments. Departments having setup their own LAN infrastructure, connecting multiple nodes at their department have been interconnected through UNIVERSITY infrastructure.

Departmental Network Guidelines would include following:

1. Access Control
2. Change Management
3. Documentation control
4. Email & Internet Usage
5. Information Security
6. IPR
7. Network Management
8. Patch management
9. Personnel