



**SRM University Delhi -NCR
Sonapat, Haryana. Acceptable
IT Use Policy V 1.1, 2022**

Central ITKM Services

SRM University (SRMUH) 2022. All rights reserved.

0/1

Delhi SRM

K. Anand

San

SRM University: Acceptable IT Use policy v1.1, 2022

AUTHOR (FOR THIS VERSION)		SRM ITKM WING			
Owner		SRM University Delhi-NCR			
Document Title		Acceptable IT Use policy v1.1,2022			
Document Reference		ITKM Policy & Guidelines			
Classification		Confidential			
version	1.1	status	For Review	Date	02-May-2022

Reviewers		
Name	Role	Organisation Unit
Mr. Balasundararaj.P	IT & Projects	ITKM
Mr.Manoj Madhavan Kutty	Coordinator ITKM	Administration

Approvers		
Name	Role	Organisation Unit
Prof.V.Samuel Raj	Registrar	Administration

of

D-V-S-M

K. Arudachari

Sam

DISCLAIMER

SRM University reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of SRM rules or policies.

SRM also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.

While SRM will make all reasonable efforts to ensure privacy and confidentiality of user data and availability of service to users, SRM disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

SRM also reserves the right to amend these policies at any time without prior notice and to take action as necessary or appropriate to comply with applicable laws.

D-V-S-M

K. Andhaya

Hi

San

Table of Contents

1	COMPUTING RESOURCES.....	5
1.1	APPLICABILITY	5
1.2	RIGHTS & RESPONSIBILITIES	5
1.3	GENERAL GUIDELINES	5
1.4	SECURITY & PRIVACY.....	6
1.5	SUPPORTED SOFTWARE	7
1.6	PROHIBITED DOWNLOADS	8
1.7	ENFORCEMENT	8
2	E-MAIL POLICY	9
2.1	OBJECTIVE	9
2.2	EMAIL POLICY FOR FACULTY AND STAFF.....	9
2.3	POLICY FOR E-MAIL TO STUDENTS.....	10
2.3.1	General Guidelines.....	10
2.3.2	Assignment of student accounts.....	10
2.3.3	Use of student accounts.....	10
2.3.4	Forwarding of E-mail.....	10
2.4	E-MAIL ADDRESS CREATION, DISPOSAL AND RETENTION POLICY.....	10
2.4.1	Purpose.....	10
2.4.2	Employee & Student Accounts	11
2.4.3	Encrypted Communications	11
2.5	E-MAIL LIST POLICY	11
2.5.1	Overview	11
2.5.2	Purpose.....	11
2.5.3	Scope.....	11
2.5.4	Policy	11
3	COMMERCIAL USE POLICY.....	12
4	WEB PAGES POLICY	12
5	COMMERCIAL PAGES POLICY	13
6	EXTERNAL LINKS POLICY	13
7	EXCESSIVE OR DISRUPTIVE USE POLICY	13
8	NETWORK INFRASTRUCTURE/ROUTING POLICY	13
9	WIRELESS POLICY	13
10	VIRTUAL PRIVATE NETWORK (VPN) POLICY	14
11	ENCRYPTION POLICY.....	14
11.1	DEFINITIONS	14
11.2	PURPOSE	14
11.3	SCOPE.....	14
11.4	POLICY.....	14
11.5	ENFORCEMENT	14
12	NETWORK TRAFFIC PRIORITIES	15

Handwritten signature

D.V.C.M

K. Anand

Handwritten signature



13	NOTEBOOK/LAPTOP SECURITY	15
13.1	PURPOSE	15
13.2	SAFETY AND SECURITY GUIDELINES	15
14	PASSWORD POLICY	16
14.1	DEFINITIONS	16
14.2	OVERVIEW	16
14.3	PURPOSE	16
14.4	SCOPE.....	16
14.5	POLICY.....	17
14.5.1	General.....	17
14.5.2	Application Development Standards.....	17
14.5.3	Use of Passwords and Passphrases for Remote Access Users	18
14.6	ENFORCEMENT	18
15	GUIDELINES FOR INTERNATIONAL STUDENTS	18
16	USING SRM_NET.....	19
16.1	USE DHCP TO OBTAIN AN IP ADDRESS AUTOMATICALLY	19
16.2	USING WIRELESS	19
17	RESPONSIBILITIES OF UNIVERSITY ITKM WING.....	19
17.1	MAINTENANCE OF COMPUTER HARDWARE & PERIPHERALS.....	19
17.1.1	Scope of Service.....	19
17.2	MAINTENANCE OF NETWORK.....	19
17.3	MAINTENANCE OF SERVER.....	20
17.4	RESPONSIBILITY FOR ITKM HELPDESK	20
18	RESPONSIBILITIES OF THE ADMINISTRATIVE UNITS	21
19	VIDEO SURVEILLANCE POLICY	21
19.1	THE SYSTEM	21
19.2	PURPOSE OF THE SYSTEM	22
20	PROCUREMENT & MANAGEMENT POLICY	24
20.1	PROCUREMENT POLICY	24
20.2	MAINTENANCE/UPGRADATION POLICY	25
20.3	POLICY FOR WRITING-OFF ITKM EQUIPMENT.....	26
21	OWNERSHIP.....	26

D.V.S.M

K. Anandija

Son

Acceptable IT Use

1 Computing Resources

As part of its educational mission, the SRM University Delhi-NCR (SRMUH) acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research and service missions; University administrative functions; student and campus life activities; and for free exchange of ideas within the University community and wider local, national, and world communities.

1.1 Applicability

- i. This policy applies to all users of University computing resources, whether affiliated with the University, and for use of those resources, whether on campus or other remote locations.
- ii. "Users" are defined as anyone who uses University systems or networks including employees, students, parents, vendors, contractors, support personnel etc.

This policy also governs specific computers, computer systems or networks provided or operated by specific units of the University. This policy may be modified as deemed appropriate by the University from time to time as posted on the University's Intranet.

1.2 Rights & Responsibilities

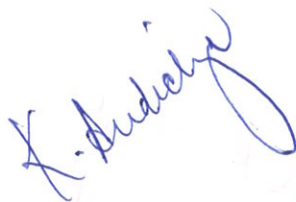
The right of academic freedom and freedom of expression applies to the users of University computing resources. So do the responsibilities and limitations associated with those rights. While the University's campus and computing environment will be open to free expression of ideas, including unpopular points of view, the use of its computing resources, like the use of other University-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible.

1.3 General Guidelines

- i. Users of University computing resources shall comply with applicable national laws, applicable State Laws, University rules and policies, and the terms of applicable contracts including software licenses while using University computing resources. Examples of applicable laws, rules and policies include the laws of privacy, copyright, trademark, obscenity and child pornography; the **IT Act 2000**, which prohibits "hacking," "cracking" and similar activities.
- ii. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. For further clarifications, users should contact the Head ITKM (CIO) or Registrar or the Vice Chancellor, SRM University for more information.
- iii. Users will be required to obtain necessary authorizations before using University computing resources. Any hardware/physical asset issued to a user must not be tampered with or given



D.V.S.M



- for repair/replacement outside of University authorized vendors. If emergency off-campus repairs are warranted, prior approval should be taken from the IT Manager at the users base location. Users will also be responsible for any activity originating from their accounts which they are reasonably expected to control.
- iv. For any loss/damage of issued assets, the University will bear losses up to Rs. 5,000/- (rupees five thousand only) for the duration of the users service. A record will be kept of such losses and if the above limit is exceeded, appropriate disciplinary enforcement shall apply. Any insurance claim amounts that are received will offset the negative balance to the extent of Rs. 5,000/- (rupees five thousand only).
 - v. Accounts and passwords should not, under any circumstances, be used by persons other than those to whom they have been assigned by the systems administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate systems administrator, and/or Dean, Director, or Department Head.
 - vi. While no set bandwidth, disk space, CPU time, or other limit are applicable to uses of University computing resources, the users are required to limit or refrain from specific uses if, in the opinion of the Head ITKM (CIO), such use interferes with the efficient operations of the system.
 - vii. Users should not state or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so. Authorization to use University trademarks and logos on University computing resources may be granted only by the Office of Corporate Relations. The use of appropriate disclaimers is encouraged.
 - viii. Users shall not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of SRM computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs.
 - ix. Users should not bring personal mass storage devices into the University network and should not use such devices to store official data for backup purposes. Designated backup locations and procedures should be used for this purpose (Drive X: provided to all campus users). Deliberate attempts to circumvent data protection or other security measures will be dealt with seriously. All data that is deemed important / critical from an organization perspective should be copied on the users X: Drive at the end of each working day. This includes but is not limited to informational lists, emails, presentations, documents, internal memos, and external communication. Following this procedure ensures that there is a retrievable copy of the data should any unforeseen eventuality occur on the users machine. Data on Drive X: is regularly backed up on central systems.

1.4 Security & Privacy

- i. While the University employs various measures to protect the security of its computing resources and its user's accounts, it cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly as well as storing critical data in University defined storage locations.

Shi

K. Anandhalingam

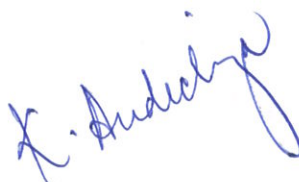
D.V.S.M

San

- ii. Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The University may also specifically monitor the activity and accounts of individual users of University computing resources, including individual login sessions and the content of individual communications, without notice, when:
- The user has voluntarily made them accessible to the public, as by posting to a newsgroup or a Web page;
 - It reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability;
 - There is reasonable cause to believe that the user has violated or is violating this policy;
 - An account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.
- iii. Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, shall be authorized in advance by the appropriate Dean / Director or the Head ITKM. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University authorities or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made through University computing resources will also be generally subject to the **Indian IT Act, 2000** to the same extent as they would be if made on paper.
- iv. Visitors to SRM Web sites who are not currently SRM students, faculty or staff should refer to the University's Disclaimer and Terms of Use for privacy information.

1.5 Supported Software

- i. Unless otherwise specified, the following is a list of software approved by the University and supported by central IT. These applications will be installed and maintained for all security patches and updates on computers owned by the University:
- a. Base Operating System (Microsoft Windows)
 - b. Office Automation Suite (Microsoft Office)
 - c. Acrobat Reader and generator (if required)
 - d. File compression utility
 - e. Email client
 - f. Web Browser (Microsoft Internet Explorer / Mozilla Firefox or Google Chrome)
 - g. Antivirus software (Kaspersky)
 - h. Licensed Domain specific software on lab computers
 - i. Rich media players (VLC or Quicktime)



- j. E-book readers (Microsoft, Kindle or other standards compliant reader).
- ii. Any software installation in machine has to be done after due approval from the office of ITKM. Any software installed without knowledge of ITKM will be treated as an information security breach and consequent losses of data/information will be the responsibility of the owner. Central ITKM assumes no responsibility for the correct functioning of the user's PC or safety of their data, should such applications cause damage to the files / data.

1.6 Prohibited downloads

The following downloads are specifically not allowed on computers unless approved in writing by Central ITKM:

- i. *Any peer to peer file sharing application:* Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications – called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer.
- ii. *Any third party personal antivirus or firewall:* Since adequate security has already been provided for on all machines via pre-defined firewall rules, third party firewalls may interfere with these rules thus endangering the network.
- iii. *Any third-party screen saver or wallpaper:* This is to prevent images that might be deemed offensive by some users from being displayed on monitors. Users should use the default screen savers available on their local machines.
- iv. Firewall, Content Filter, Vulnerability assessment, End Point protection are provided by the university and are deployed to ensure compliance to the security of the entire IT infrastructure.
- v. *Hacking tools of any sort:* The use of any such tools on University machines is strictly prohibited.
- vi. *Games & Movie trailers or previews:* These provide no productive academic benefit and have a tendency to affect productivity, and hence are not allowed on University machines. Users who use their own local machines / University provided portables on which to work are exempt from this policy. For this purpose, games could be in any form – executables or flash based games downloaded from the Internet.

1.7 Enforcement

- i. Users found violating this policy may be denied access to University computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal.
- ii. Alleged violations will be handled through the University disciplinary procedures applicable to the user.
- iii. The University may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability.
- iv. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Shi

K. Anudechya

D. V. S. M

San

- v. General enforcement applicable If a user is found in violation of the above, will be:
- First time offence – Account suspension for one week (7 working days) unless countermanded in writing by the Administrative Head of the location as applicable to the user.
 - Second time offence – Account suspension for two weeks (14 working days) subject to the above provision.
 - Repeat offences – information to the applicable disciplinary process for suitable action.

2 E-Mail policy

2.1 OBJECTIVE

For purposes of this document, e-mail includes point-to-point messages, postings to newsgroups and list serves and any electronic messaging involving computers and computer networks. Organizational e-mail accounts, including those used by student organizations, are held to the same standards as those for individual use by members of the University community. E-mails are also generally subject to the **IT Act, 2000** to the same extent as they are on paper.

Examples of Inappropriate Uses of E-mail:

- a. The following uses of e-mail by individuals or organizations are considered inappropriate and unacceptable at the SRM University Delhi-NCR. In general, e-mail shall not be used for the initiation or re-transmission of:
- i. Chain mail that misuses or disrupts resources - E-mail sent repeatedly from user to user, with requests to send to others;
 - ii. Harassing or hate-mail - Any threatening or abusive e-mail sent to individuals or organizations that violates University rules and regulations;
 - iii. Virus hoaxes;
 - iv. Spamming or e-mail bombing attacks - Intentional e-mail transmissions that disrupt normal e-mail service;
 - v. Junk mail - Unsolicited e-mail that is not related to University business and is sent without a reasonable expectation that the recipient would welcome receiving it; and
 - vi. False identification - Any actions that defraud another or misrepresent or fail to accurately identify the sender.
- b. The University may add more such inappropriate uses from time to time as deemed necessary.

2.2 Email Policy for Faculty and Staff

Email services are provided to faculty and staff members for the tenure of their engagement with University. Once the tenure is over, members will not have access either to email services or to the content stored in their respective mailboxes. IT services will create and discontinue individual member email addresses basis inputs provided by Human Resources department. This is the official email addresses of members which will be listed in University Directory and other appropriate publications.



2.3 Policy for E-mail to Students

The SRM University Delhi-NCR (SRMUH) utilizes e-mail as one of the official means of communication with students to keep them informed of important information such as financial aid and billing data; college deadlines, events and updates; and important campus news. Each student is issued an official e-mail account for use while he or she is enrolled.

2.3.1 General Guidelines

E-mail is an appropriate and preferred method for official communication by SRM with students unless otherwise prohibited by law. The University reserves the right to send official communication to students by e-mail with the assumption that students will receive, read and, if necessary, act in a timely manner based upon these e-mails.

2.3.2 Assignment of student accounts

Upon confirmation of admission to SRM, a University e-mail account is automatically created for each student in the form of initialslastname.year@stu.srmuniversity.ac.in or as otherwise determined by IT Services. Official e-mail accounts are maintained by IT Services and will be published online and in the student directory. This e-mail address remains with the student throughout their academic career at SRM University as well as afterwards should the student choose to use it.

2.3.3 Use of student accounts

- i. It is the responsibility of students to access and maintain these accounts in accordance with other University electronic communication policies including, but not limited to, the Acceptable Use Policy.
- ii. Students are expected to check their email on a frequent and consistent basis. Students must make sure that there is sufficient space in their accounts to allow for e-mail to be delivered and have the responsibility to recognize that certain e-mails may be time sensitive. Students will not be held responsible for an interruption in their ability to access a message because of system problems that prevent timely delivery of, or access to, messages. These include scheduled and unscheduled outages of the system.

2.3.4 Forwarding of E-mail

Students who choose to have their email forwarded to an unofficial e-mail address will do so at their own risk. SRM is not responsible for any e-mail beyond delivery to SRM official accounts. Students are however responsible for official e-mail as outlined above.

2.4 E-mail address creation, disposal and retention policy

2.4.1 Purpose

- i. This e-mail Policy is intended to help faculty, staff, and students understand when and how their accounts are created and determine what information sent or received by email should be retained and for how long.



- ii. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.
- iii. All Faculty, Staff, and Students should familiarize themselves with this eMail policy.
- iv. Questions about the proper retention of a specific piece of information should be addressed to the users administrative reporting officer.
- v. Questions about these guidelines should be addressed to the eMail Administrator or HOD ITKM.

2.4.2 Employee & Student Accounts

- i. Faculty/Staff accounts are created when new employees are entered into the HR system. Their accounts will be available for use the day after they are entered into HR. An individual can contact the IT Services helpdesk to obtain their user name.
- ii. Deactivation - Faculty/Staff accounts will be deactivated when they are changed to an "inactive" status in HR and have no other role in ERP (e.g. also not a student).
- iii. Student accounts will be deactivated from the system when their status in ERP changes to inactive – either by reason of graduation or withdrawal from the University.

2.4.3 Encrypted Communications

- i. SRM encrypted communications should be stored in the following manner:
 - a. The encryption standard used should be 128 bit encryption.
 - b. Bitlocker is used in all critical machines for encryption.
- ii. In general, information should be stored in a decrypted format – unless deemed sensitive by the University.

2.5 E-mail list policy

2.5.1 Overview

Management of e-mail lists is an important service to assist University constituencies communication efforts. As such, all University IT Services users are responsible for understanding the types of lists available and for following defined processes for requesting e-mail lists.

2.5.2 Purpose

The purpose of this policy is to establish standards for E-Mail Lists.

2.5.3 Scope

The scope of this policy includes all IT Services personnel.

2.5.4 Policy

- A Request must be created for new e-mail list requests in the Helpdesk, regardless of first point of contact.
- A Technical Support Specialist shall be assigned to work with user requesting the e-mail list to determine specifications and, if the request is approved, provide training once the list is established



- If the list is for one area or the requestor provides a specific set of e-mail addresses, the request will be approved; however, if the request crosses functional/departmental areas or requests "all" users the request must be routed through the appropriate office.
- Lists including on-campus e-mail addresses only and does not require the functionality of a listserv will use a distribution list that is maintained in the Global Address Book.
- Lists including off-campus e-mail addresses or a combination of on and off-campus addresses will use third party applications.
- All lists will have a user as a "list administrator" assigned; the administrator is the person from the area/group requesting the list.
- Both types of e-mail lists are maintained by the administrator of the list, not by IT Services..

3 Commercial Use Policy

- i. Computing resources are not to be used for personal commercial purposes or for personal financial or other gain.
- ii. Occasional personal use of University computing resources for other purposes may be permitted provided it does not lead to excessive use of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy.
- iii. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

4 Web Pages Policy

- i. Official University pages (including colleges, departments, bureaus, centers, institutes, etc.) represent the University and are intended for the official business functions of the University.
- ii. Each official home page must use an address that ends in ".SRMUniversity.ac.in" and be registered with the University's Web administrator who will then include it as a link from the SRM Website or intranet.
- iii. The following information must be readily accessible on the main page:
 - a. The name of the unit or group represented by the page;
 - b. Contact details of the person(s) responsible for maintaining the page content;
 - c. Date of last revision;
 - d. The unit logo (if separate from the University logo); and
 - e. An active link to the SRM home page.
- iv. Faculty and staff who wish to publish substantial personal information not related to their University functions should use an Internet service provider rather than using University Web resources.
- v. User posting on official University forums / Social media accounts must be done in a personal capacity and must not contain / disclose any confidential/proprietary information. They should not be derogatory, inflammatory, or insulting to any member of the University community or to any other user, or based on fallacious facts. It should be noted that such postings are the user's personal opinion and do not represent the University's views in any way. It is the University's prerogative to suitably amend/remove posts that do not conform to the above as

Shi

K. Andrichy D.V.S.ith

San

well as initiate disciplinary action against the poster- including and up to termination of services.

5 Commercial Pages Policy

- i. Using SRM Web pages for personal gain is forbidden. Any private commercial use of SRM Web pages must be pre-approved pursuant to existing University policies and procedures regarding outside employment activities.
- ii. All SRM units that accept payment electronically via the Internet are required to process all such transactions through the approved payment gateway.

6 External Links Policy

SRM University accepts no responsibility for the content of pages or graphics that are linked from SRM pages. However, Web page authors should consider that such links, even when clearly labeled, can be misinterpreted as being associated with the University. Links to pages where users have a personal monetary interest are likely to violate policies regarding advertising and commercial use and should be avoided.

7 Excessive or Disruptive Use Policy

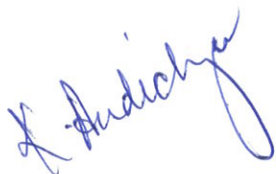
Excessive or disruptive use of University resources in the viewing or publishing of Web pages is not permitted. Colleges, Departments, or Centres owning or administering the resources involved will determine whether specific usage is considered normal, excessive or disruptive.

8 Network Infrastructure/Routing Policy

- i. Users must not attempt to implement their own network infrastructure including, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to SRM IT resources such as modems and virtual private networks (VPNs).
- ii. Users must not offer network infrastructure services such as DHCP and DNS. Exceptions to this policy must be coordinated with the local network administrator with prior approval from the Manager-IT.

9 Wireless Policy

- i. For the purposes of this document, we refer only to wireless transmission using radio frequency (RF). As wireless is a shared media and easily intercepted by a third party, wireless users are encouraged to use some type of encryption. Use of the **WPA2-AES** or **WPA2-TKIP** encryption protocols is suggested to encrypt wireless communication.
- ii. Improperly configured wireless access points (WAPs) might cause denial of service to legitimate wireless users and can also be used to subvert security. Wireless access points must be authorized by the Systems Administrator.



10 Virtual Private Network (VPN) Policy

- i. A VPN provides secure encrypted access between a client and the VPN server. They are most commonly used to secure access to a trusted network from remote, untrusted networks.
- ii. VPN servers must be authorized by the Manager IT.

11 Encryption policy

11.1 Definitions

Proprietary Encryption: An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

11.2 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have been proven to work effectively.

11.3 Scope

This policy applies to all SRM users and affiliates.

11.4 Policy

- i. University faculty and staff are encouraged to encrypt files, documents, and messages containing sensitive or confidential University information for protection against unauthorized disclosure while in transit.
- ii. However, any encryption performed on University systems must use proven standard algorithms and such encryption must permit properly designated University officials, when required and authorized to decrypt the information.
- iii. Proven, standard algorithms should be used as the basis for encryption technologies. Examples of standard encryption tools include:
 - Pretty Good Privacy (PGP), which uses a combination of IDEA and RSA or Diffie-Hillman.
- iv. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Information Technology Services.

11.5 Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

oli
K. Andeche
D-V-S-ih
Sa

12 Network traffic priorities

IT Services uses a network utility to control and prioritize the types of traffic on the University's Internet connection.

The university network priorities are as listed below:

- a) Academic infrastructure and applications.
- b) Enterprise applications.
- c) Collaboration applications.

13 Notebook/Laptop security

13.1 Purpose

This procedure describes security measures required to protect portable information assets (and the information that resides on these devices) such as notebook or tablet computers, personal digital assistants (PDA's), CDs, flash drives, DVDs, pagers, cell phones or other similar equipment from theft, loss or damage. Each user must follow the requirements for protecting University information, as set forth in SRM University Information Sensitivity Policy (restricted to campus).

13.2 Safety and Security Guidelines

The practices listed below do not cover all potential risks, but will significantly minimize the likelihood of theft, loss or damage to University equipment and information. They may apply to one type of device and not another; the user is responsible for applying the measures appropriate to the device.

- i. If you travel with a notebook, make sure that you have the notebook case, including all its contents, over your shoulder before you leave the plane, taxi or train. When passing through a security checkpoint, keep your eyes on the device and pick it up as soon as possible.
- ii. Make a record of the make and model of the notebook and any serial or company identification number on the equipment and store the record in a separate safe place.
- iii. If you must leave a notebook or other device in a vehicle, put it out of sight and lock the vehicle or lock it in the trunk. Do not leave equipment in the vehicle at all in very cold or very hot weather, as extreme temperatures may cause damage.
- iv. In an office or work area shared with others, or in an area accessible by the public, either secure the notebook, or other device, or keep it with you at all times. Never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the notebook and any other sensitive material in a locked drawer or cabinet.
- v. Back up your data frequently and store the files in a safe location separate from the notebook or other device.
- vi. Encrypt or password-protect each file containing confidential and/or sensitive University information. Make passwords difficult to crack. A mixture of special characters, numbers, and upper and lower case letters is considered the most secure — but only if passwords are not

Handwritten initials

Handwritten signature: D.V. Ch

Handwritten signature: K. Arudhyan

Handwritten signature: San

stored on the hard disk. If your notebook comes with biometrics software (such as fingerprint imaging) configure the notebook to use it.

- vii. Sensitive and/or Critical information includes, but is not limited to:
- All information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni) including but not limited to dates of birth, personal contact information student education records, medical information, benefits information, compensation, loans, financial aid data, alumni information, donor information, and faculty and staff evaluations.
 - The University's proprietary information including but not limited to intellectual research findings, intellectual property, financial data, and donor and funding sources.
 - Information, the disclosure of which is regulated by government
- viii. Restrict plug and play. Plug and Play is convenient, but can sometimes be dangerous: if someone connects a USB flash drive, MP3 player or external hard disk drive to a notebook, it is recognized automatically — and it is then easy to start exporting data.
- ix. If your notebook is lost or stolen file an FIR with the Police and report the device's serial number as lost or stolen to the IT Services Help Desk.

14 Password Policy

14.1 Definitions

Application Administration Account

Any account that is for the administration of an application (e.g., Oracle database administrator, ERP administrator).

14.2 Overview

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of the entire University's network. As such, all University students and users (including contractors and vendors with access to University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

14.3 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

14.4 Scope

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University facility, has access to the University network, or stores any non-public University information.

07i

K. Andealya

D. V. S. M.

Sa

14.5 Policy

14.5.1 General

- i. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.
- ii. All production system-level passwords must be part of the IT Services administered global password management database.
- iii. All user-level passwords (e.g., email, web, desktop computer, etc.) must have
 - a. Maximum password age of 180 days
 - b. Minimum password age of 2 days
 - c. Exhibit complexity by
 - i. Not containing all or part of the user's account name
 - ii. Contain characters from three of the following four categories:
 1. Uppercase characters (A through Z)
 2. Lowercase characters (a through z)
 3. Base 10 digits (0 through 9)
 4. Non-alphabetic characters (for example, !, \$, #, %)
 - d. Maintain a password history of 3 passwords and not allow reuse
 - e. Must be a minimum of 8 characters
 - f. Be locked out if more than 5 unsuccessful attempted logons
- iv. Applications will automatically log-offs after a predetermined period of inactivity; username and password will be required for re-authentication.
- v. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- vi. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.
- vii. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- viii. All temporary passwords must be changed at first logon.
- ix. If an account or password is suspected to have been compromised, report the incident to IT Services and immediately change all of the associated passwords.
- x. Automated password guessing may be performed on a periodic or random basis by IT Services Management or its delegates. If a password is guessed during one of these scans, the user will be required to change it.

14.5.2 Application Development Standards

Application developers must ensure their programs contain the following security precautions.
Applications:

- i. Should support authentication of individual users, not groups.

Shi

D. V. S. M

K. Indira

San

- ii. Should not store passwords in clear text or in any easily reversible form.
- iii. Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- iv. Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

14.5.3 Use of Passwords and Passphrases for Remote Access Users

Access to the University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

14.6 Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15 Guidelines for International students

Foreign students are defined as holders of passports of countries other than India. For such students, the rules, policies and procedures as described in this document will be applicable. However, additionally the following would also apply:

- i. The student ids will be given a broader degree of access to the Internet. Specifically, this access would include access to all websites (except pornographic in nature) without any debarring of any kind of sites, and access to Voice/video over IP facilities such as Skype.
- ii. Access and support on mobile devices such as smartphones, tablets etc.
- iii. Should the student have any application or device that is not covered by (a) and (b) above, the student should approach the IT Operations in-charge at their respective campus and provide specifics about the application / device. All reasonable efforts would be made to enable access for the same within the framework of the rules.

Additionally the students are advised to ensure the following on their device:

- i. Ensure your operating system (OS) (Windows or otherwise) is legal
If you are using an "illegal" (unpaid, borrowed, or otherwise unlicensed) copy of Windows or other OS, your network login will not be successful and you will not be able to use SRMNET until that issue is resolved. If you have a PC with Microsoft Windows, you should bring legal Windows software CDs with you to the University, or you may have trouble connecting to the network.
If you do not already have legal Windows CDs, please purchase Windows before you leave your home country (and bring your Windows CDs with you)
OR
be prepared to purchase an English-language version of Windows when you arrive.
- ii. Make sure you are running the current Windows service pack
Once you do have a "legal" version of Windows, you should turn on Automatic Updates and allow any updates that you're prompted to do.
- iii. Remove viruses and spyware

Oh

R. Andulige

D. V. S. M

San

Please do what you can to remove viruses and spyware from your computer before you try to use SRM_NET.

16 Using SRM_NET

16.1 Use DHCP to obtain an IP address automatically

As a student at SRM, you should never have reason to set a static IP address. Once you have properly registered on the network, an IP address will be assigned to you. Giving yourself (or any friends you are helping) a specific IP address will disrupt your network access in the long run, even if it seems to work initially.

16.2 Using wireless

The University wireless network is accessible from most of the common areas across the campus, including hostels and other accommodation facilities. When you are on campus, the wireless SSID you should be using is SRM_NET (802.11x). You cannot run an independent wireless access point on the SRM University campus.

17 Responsibilities of University ITKM Wing

Information Technology and Knowledge Management (ITKM) wing have five inner wing i.e. Network, Server, Website (Application), ERP, Helpdesk and Hardware & Peripherals;

17.1 Maintenance of Computer Hardware & Peripherals

Information Technology and Knowledge Management (ITKM) is responsible for maintenance of the University owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

17.1.1 Scope of Service

ITKM will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

Service Request & Complaints: ITKM may receive complaints or service request through email (ithelpdesk@srmuniversity.ac.in) or by telephone.

Installation of Un-authorized Software: service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

Reporting IT Policy Violation Incidents: If ITKM or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the ITKM and the university authorities.

17.2 Maintenance of Network

- i. The campus network backbone and its active components are administered, maintained and controlled by ITKM.

0/1

A.V.S.M

K. Anand

San

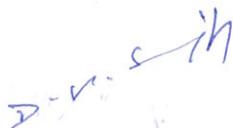
- ii. This unit operates the campus network backbone such that service levels are maintained as required by the University, departments, and divisions served by the campus network backbone within the constraints of operational best practices.
- iii. This cell will be responsible only for solving the network related problems or services related to the network.
- iv. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of this unit.
- v. Major network expansion is also the responsibility of ITKM. Every 3 to 5 years, reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by ITKM's Network unit when the university makes the necessary funds available.
- vi. Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.
- vii. This unit is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. ITKM monitors the network to ensure that such services are used properly.
- viii. This unit is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilization are reported to the ITKM technical staff for problem resolution.
- ix. It is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

17.3 Maintenance of Server

- i. To be a single point of contact for first level technical support and escalation.
- ii. Monitoring server uptime and utilization status.
 - a. Windows server. Twice a day.
 - b. Server. Twice a day
 - c. Application server. (E.g. ERP, Smart card Attendance, mail, Website). Twice a day.
 - d. Proxy server, Antivirus server etc. Twice a day.
- iii. Taking ownership of the call till closer with proper resolution.
- iv. Taking proxy violation report and discuss with ITKM.
- v. Taking support from next level technical support team.
- vi. Taking support from principal vendor.
- vii. Focus on service restoration ASAP.
- viii. Notify update and communicate the status to internal team.
- ix. Resolve cases with signed Report or mail confirmation.

17.4 Responsibility for ITKM Helpdesk

- i. ITKM Helpdesk management ensures standardized methods and procedures are used for efficient, prompt and authorized handling of all Helpdesks in the ITKM Infrastructure.
- ii. Any change or addition of an ITKM Helpdesk has to be identified and registered with the Helpdesk register through the Helpdesk management process and the procedures.
- iii. It is responsible for any Helpdesk collection, installation, addition, movement, change need to be properly documented.



- iv. To provide support for users in the use of a range of specialist digital design software packages.
- v. To provide support for users in the operation of a range of hardware including printers, scanners and other external peripherals'.
- vi. To ensure that resources within the IT suites are supported through the development of printed and online instructional material to reduce call rates and enable users to become more self-sufficient.
- vii. To deliver where required inductions and basic training in the use of IT facilities and services provided by ITKM.
- viii. To accurately record, update and document requests using the IT service desk system.

18 Responsibilities of the Administrative Units

ITKM needs latest information from the different Administrative Units of the University for providing network and other IT facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the SRMUH web site up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- Information about New Appointments/Promotions.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the university authorities that makes an individual ineligible for using the university's network facilities.
- Information on Important Events/Developments/Achievements.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on mobile storage devices or PDA or by email) should be sent to ITKM.

19 Video Surveillance Policy

19.1 The system

- i. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.
- ii. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
- iii. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
- iv. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Shi

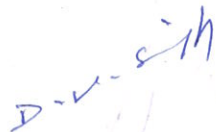
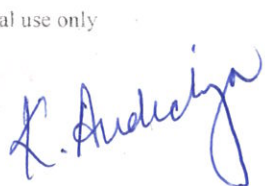
D.V.C.M.

K. Andrich

San

19.2 Purpose of the system

- i. The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:
 - Deter those having criminal intent
 - Assist in the prevention and detection of crime
 - Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.
 - Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
 - In the case of security staff to provide management information relating to employee compliance with contracts of employment
- ii. The system will not be used:
 - To provide recorded images for the world-wide-web.
 - To record sound other than in accordance with the policy on covert recording.
 - For any automated decision taking
- iii. Covert recording
 - a. Covert cameras may be used under the following circumstances on the written authorization or request of the senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer.
 - b. Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.
 - c. The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.
- iv. The Security Control Room
 - a. Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.
 - b. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry.
 - c. Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.
 - d. Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the centre. A similar log will be



- kept of the staff on duty in the Security Control Room and any visitors granted emergency access.
- v. Security Control Room Administration and Procedures
 - a. Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.
 - b. Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.
 - vi. Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.
 - vii. Recording
 - a. Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.
 - b. Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.
 - c. All hard drives and recorders shall remain the property of university until disposal and destruction.
 - viii. Access to images
 - a. All access to images will be recorded in the Access Log as specified in the Procedures Manual
 - b. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.
 - ix. Access to images by third parties
 - a. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:
 - i. Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
 - ii. Prosecution agencies
 - iii. Relevant legal representatives
 - iv. The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
 - v. People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
 - vi. Emergency services in connection with the investigation of an accident.
 - x. Request to prevent processing
 - a. An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

o/h

D-V-S-M

K. Anandhaya

Son

- b. All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.
- xi. Complaints
It is recognized that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, These rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

20 Procurement & Management Policy

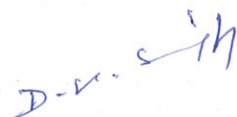
20.1 Procurement Policy

- I. ITKM is responsible to define, review, revise, approve & circulate/publish on website the procurement policy for the ICT equipment once in every year.
- II. All users/user departments must adhere to the policy guidelines published by the ITKM
- III. All users / user departments must take prior approval of authority for requirement and specifications of the ICT equipment they wish to procure.
- IV. The procurement committee should meet once every month before the purchase committee meet.
- V. The committee shall strive to standardize the terms & conditions as well as the process for the procurement of ICT equipment and software in line with the ITKM Policy and guidelines.
- VI. It must perform the vendor evaluation and registration process every two years to identify & register the vendors for the general purpose IT equipments and circulate the same to all user departments.
- VII. The procurement process should also be in accordance with accounting & auditing provisions and guidelines of the University.
- VIII. Bulk procurement by combining the requirements of similar equipment should be encouraged to achieve optimum cost benefits. Procurement of equipment / software from Original Equipment Manufacturer (OEM) vendor must be preferred.

The following aspects must get a consideration, as a part of ICT Procurement Policy:

Feasibility: If an item / technology is not already existing and is being introduced, an appropriate justification for introducing new item / technology must be prepared. It must also consider the alternate technologies explored and the reasons why the choice for the selected technology was made.

Cost Benefit: The initiator of the proposal must submit a statement of the cost – benefit expected from the procurement. In case the benefits are subjective, a subjective assessment in terms of the underlying criteria and their rankings from points 1 to 10 must be submitted. This will help the technical staff to match the requirement with the technology being procured.



Plans and Budgets: It is desirable that all Faculties and Departments plan their IT requirements in advance and provide for the same in their budgets. The budgets must cover Capital Investments as well as recurring, operational expenses. This will help in controlling the monetary outflow while enhancing the IT Resources. The specifications and configuration submitted for procurement must be consistent with the intended usage and should be derived in consultation with members of the IT Infrastructure Management Committee.

Financing: Appropriate means for financing must be available for IT Procurement. Experts in Finance at the University may appropriately suggest leasing and other means for funding the procurement appropriately. It is also desirable that a common pool is available such that in case a procurement having merit is falling short of the budget, it can supplement the budget.

Accounting: Entire ITKM Infrastructure including Hardware, Software and Communications Equipment comes at a cost and certainly needs to be accounted for accurately. These items must be treated as assets and their procurement, transfers and disposals must get reflected in the Accounts Books of Assets at any given time.

Systems Audit: There must exist a system of cross checks and physical verifications of IT Assets to ensure that all assets exist, they are functioning as expected, are technically fit and not obsolete. Such audit help in determining in advance the items that need replacements over a period of time and so, can be well planned. This activity will prevent any degradation of efficiency in the ITKM Services.

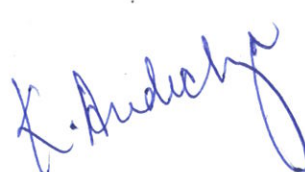
Information Security: There are different aspects of Information Security. They are broadly classified as Digital and Physical. Security related to Digital Devices is related with Passwords, Access Rights, Backups, Anti-Virus Measures, use of external media and so on. Physical Security involves securing parts of physical location to regulate its access, to restrict only authorized personnel, to provide for smoke detectors and fire alarms, to enable monitoring through CCTV Cameras and so on. On the other hand, Physical Security covers classification, storage and upkeep of documents, regulating access to classified documents and arranging for their safe custody, sharing of confidential information, inadvertent leakage of classified information and so on.

Outsourcing: In the modern world, outsourcing is beneficial and cannot be avoided but there are many aspects that need to be considered while outsourcing activities or while having external staff working within University premises. These concerns are related with providing information related with outsourced jobs, getting certain repairs done, disposing off items / equipment and so on – all of which must be carefully carried out considering IT Security and safety in mind. Similar care should be taken while executing any turn-key projects in the area of IT implementation.

Best Practices: There must be personnel earmarked to keep abreast of the developments in Technology, who must be assigned the identification of appropriate avenues wherein new technology /products may be profitably deployed. They must also keep themselves aware about the Best Practices desirable and / or being followed elsewhere, which may be beneficial to the University.

20.2 Maintenance/Upgradation Policy

On procurement & installation of any new IT device/equipment, User department must allocate a unique dead-stock number (Asset Identification Number) in the deadstock/Asset Register. The same number must be written on the front side of the device/equipment, which can be used for physical



verification. The same must be appropriately updated while transferring out OR disposing/writing off such assets.

User department must be vigilant about warranty checks and must take appropriate action if the performance of the device/equipment deviates from the expected performance.

After the completion of the warranty period, User Department may implement the Annual Maintenance Contract (AMC) for the device/equipment depending on the criticality of its usage, with the approval of the ITKM Infrastructure and Management Committee & following the standard procedure laid down by the University from time to time.

The ITKM Infrastructure and Management committee shall define, review, revise, approve and circulate/publish the guidelines & procedure for up-gradation of outdated ICT devices/equipments/components or to improve the performance of existing IT devices/equipments/components and software. The upgradation of devices/equipments can be through increasing the performance capacity by adding/replacing some components, like memory, HDD, Graphic card etc. or by replacing the whole device/equipment through a buy-back mechanism depending on the specifications and performance parameters of the device/equipment. A prior approval of specifications and requirement by the ITKM is essential

Necessary budget provisions must be made by the respective user departments for the maintenance and up-gradation of its IT equipment and software.

20.3 Policy for Writing-Off ITKM Equipment

ITKM is responsible to define, review, revise, approve and circulate/publish the guidelines & procedure to scrap and write off the non-functional, non-operable, non-repairable and obsolete ITKM devices/equipments.

It must perform the vendor evaluation and registration process to identify & register the vendors specialized in disposal of e-scrap or digital scrap.

21 Ownership

ITKM has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

