IIS (Deemed to be University)

IT Policy

(Revised-2020)

IISU Campus, Gurukul Marg, SFS, Mansarovar, Jaipur- 302020

IT POLICY

Table of Contents

Chapter 1

1. Introduction

1.1 Preamble

Among the key strategic objectives identified by the University in its vision towards excellence, is the support and development of the ICT function within the University. In this connection, one of the objectives of the IT Planning & Monitoring Committee of the University, is to maximize student and staff productivity and service delivery, enhance teaching and learning and improve quality of research through ICT. This is a challenge that requires a clear vision and commitment from all concerned including students, staff and management. The committee, acting on behalf of the University has taken its mandate of developing a blueprint that will guide in the development, implementation, and effective use of the IT services at the University. This policy will serve, alongside other related published documents, as the reference document on IT standards, where there is no separate IT standards document for the University,

1.2 Statement of Purpose

The University - IT Policy is an effort to:

- Set up procedure and guidelines to use Information Technology (IT) ensuring safety and security of personal data.
- Put up checks on the misuse of technology within the framework and provisions under the national laws & policy on the subject matter of IT

1.3 Scope of the University IT Policy

The University needs to collect, receive, possess, store, deal and handle the information and ensure the confidentiality of both the information and the information provider. The IT Rules provide for the requirement of a privacy policy for handling of or dealing with the personal information including sensitive personal data or information and ensure that the same are available for being viewed by such information providers who have provided such information under lawful contract.

The policy shall be published on the Website of the University for –

1) Clear and easily accessible statements of its practices;
2) Purpose of collection and usage of such information;
3) Disclosure of information including sensitive personal data or information; and
4) Reasonable security practices and procedures

1.4 Authority of this Policy Document

This policy document was initiated in June 2013. The policy was uploaded on the University's Website in February 2014 after taken into consideration the recommendations arising from the experts from Computer Science and IT field. This document is designed by the Department of Computer Science & IT of the University.

1.5 Definitions —

(1) In this policy (unless otherwise stated) –

(a) "Act" means the Information Technology Act, 2000 (Central Act No. 21 of 2000) as amended in 2008;

(b) "Biometrics" means the technologies that measure and analyze human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;
(c) "Cyber incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable fiber of security policy resulting in unauthorized access, denial of service or disruption or unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;
(d) "Data" means data, as defined in clause (o) of sub-section (1) of section 2 of the Act;
(e) "Information" means information, as defined in clause (v) of sub-section (1) of section 2 of the Act;
(f) "Intermediary" means an intermediary, as defined in clause (w) of sub-section (1) of section 2 of the Act;
(g) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;
(h) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with the University, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them as mentioned in the Act.

Sensitive personal data or information

Sensitive personal data or information of a person means such personal information which consists of information relating to –

(a) Password;
(b) Financial information such as Bank account or credit card or debit card or other payment instrument details;
(c) Physical, physiological and mental health condition;
(d) Sexual orientation;
(e) Medical records and history;
(f) Biometric information;
(g) Any details relating to the above clauses as provided to the University for providing service; and
(h) Any of the information received under above clauses by the University for processing, storage and being used under lawful contract or otherwise:

provided that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Chapter 2

2. Network Development and Management Policy

2.1. Objectives of network policy

(a) The objective of this policy is to establish a comprehensive and uniform Network Development and Management policy for the management of ICT infrastructure for the University.

(b) This policy defines the arrangements and responsibilities for the development, installation, maintenance, and use and monitoring of the University's ICT networks to ensure that, these networks are sufficiently adequate, reliable and resilient to support continuous high levels of activities.

2.2 Scope of network policy

This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of the University. These include all University staff and students; any other organization accessing services over University ICT networks; persons contracted to repair or maintain the University's ICT networks; and suppliers of network services.

2.3 General network policy

2.3.1 The Network

The University will develop and support a University-wide ICT network as a basic infrastructure service for the facilitation of sharing electronic information and resources by all members of the University. This includes all staff and students of the University, and other persons engaged in legitimate University functions as may be determined from time to time.

2.3.2 Universal availability

(a) The University network will be designed and implemented in such a way as to serve those located at the University campuses and, to a lesser extent, those located elsewhere.

(b) The ultimate goal is that every room in the University in which research, teaching or support activities take place should be connected. And every member of the University should have capability to access the University ICT infrastructure.

(c) The University network will form part of the general infrastructure of the University.

(d) There will be one coherent network supporting access to all general information services provided to the University members. There may be separate private networks where they are warranted.

2.3.3 Reliability

(a) High levels of availability, reliability and maintenance will be major objectives in the construction and operation of the University ICT network.

(b)The design and construction of the University network will take into account emerging technologies and standards wherever possible.

2.4 University IT Infrastructure Development

The IT Planning & Monitoring Committee will prepare a network development plan, advising on appropriate developments aimed at ensuring the adequacy of the University's ICT infrastructure in future. This plan will take account of the University's strategic plan; usage and demand patterns; technological change; security; management and cost implications. It will formulate, reviewing and monitor design strategies for development of IT infrastructure, its maintenance and record keeping of Audio Visual aids within the University campus.

2.4.1 Constitution of IT Planning & Monitoring Committee

- The committee constitution will be effective for a period of two years.
- It will meet for at least two times in an academic year.
- 50% of the total members of the Committee shall constitute the quorum for the meeting of the committee.

The constitution of the committee is:

- Convenor
- Two or three senior faculty members from Department of CS & IT/Physics/Mathematics
- Software Engineer
- Network Administrator
- One Lab Administrator
- One external member form Industry/Academics
- Member Secretary (Senior faculty from Department of CS & IT)

2.5 University Network

2.5.1 Definition

The University network will consist of several parts: a collection of inter-building connections; Campus LANs and a number of Servers. The University Network Backbone will comprise an inter-building cabling system, together with one or more "Gateway" interfaces at each building or in the path to each building which will connect the Backbone to the network(s) within each building.

2.5.2 Structure

(a) The planning, installation, maintenance and support of the University Network shall be under the control of the Network Centre.
(b) Connection to the University Network shall be approved by the Vice Chancellor of the university.
(c) The University Network at any particular point of time will be aimed at facilitating the traffic flow between connected buildings or networks.

2.6 Access to ICT facilities

2.6.1 ICT Network equipment

Entry to server room(s) and cabinets, and interference with ICT network equipment is strictly prohibited. Only designated members of the staff of Computer Center are

authorized to install and maintain active network equipment including hubs, switches and routers connected to the University's ICT networks.

2.7 Connection to and Usage of ICT facilities

2.7.1 Connecting to the IT network

(a) All connections to the University's ICT networks must conform with the requirements that apply to Internet Protocol (IP) addresses.
(b) Only designated members of staff, authorized specifically by the management, may make initial connections of desktop services equipment to the ICT network.

2.7.2 Suspension and/or termination of access to ICT networks

• University Employees

(a) A staff's access to the University's ICT networks will be revoked automatically:
i. at the end of his or her employment or research contract;
ii. at the request of his or her Dean of Faculty/Head of Resource Centre/Head of Department or Head of Unit;
iii. where he or she has breached the concerned regulations.

• Students leaving the University

The Academic Registrar will notify the Network Centre, by means of the regular student data transfer, of the names of students leaving the University so that such students' computing, e-mail, printing and lending accounts can be deleted.

2.7.3 Internet Protocol (IP) addresses

(a) All equipment connected to the ICT networks shall be assigned unique IP addresses.
(b) The IP addresses assigned to equipment shall be recorded visibly on the casing of the equipment.
(c) The Network Administrator shall plan and allocate Blocks of IP addresses to different network segments and update the IP address master record.
(d) The Network Administrator shall maintain a central record of IP addresses and may remove inactive IP addresses after six months.

2.7.4 Inventory Control

As part of their audit responsibilities, Officer-in-charge shall be required to record in their local equipment inventory records, the IP address assigned to each item of equipment for which they are responsible, together with the location of such equipment.

2.7.5 Web filtering

The Network Administrator shall be responsible for the implementation of appropriate filtering facilities for web based and non-web Internet traffic, including MP3 traffic and other high bandwidth intensive services that may not have direct educational or research value, where and when necessary in conformity with the ICT.

2.8 Monitoring of network performance

The Network Administrator shall monitor and document network performance and usage and shall maintain regular reports.

2.9 ICT Usage Policy

This policy outlines the responsible use of the ICT Infrastructure for all the users of the University. All users of the University will be subject to the following **Acceptable Use Policy:**

(a) **Academic Use:** I understand that the IT infrastructure at IIS (Deemed to be University) is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

(b) **Identity:** I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use IIS (Deemed to be University) IT resources to threaten, intimidate, or harass others.

(c) **Privacy:** I will not intrude on privacy of anyone. In particular, I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

(d) **Monitoring:** I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the IIS (Deemed to be University) administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize the University administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of the University network.

(e) **Viruses:** I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, and other similar programs.

(f) **Penalties:** I understand that any use of IT infrastructure at IIS (Deemed to be University) that constitutes a violation of the University Regulations could result in administrative or disciplinary procedures.

Chapter 3

3. IT Service Management Policy

3.1 Objectives of IT Service Management Policy

The primary focus of IT service management is the application of the best IT practices to enable IT to be a more effective service provider across the organisation. The University aims to:

- To promote IT based online teaching-learning pedagogies/methodologies and examination facility.
- To promote IT procedures at department level.

The users are students, alumnae, parents and the university employees.

The university has a specialized team to look after management of IT services, inside and outside of the university.

Some of the primary services provided to the users using **web based IT solution** are:

- Attendance
- no dues form
- examination form submission
- permission letter
- assignment
- events
- results
- admission form
- email

3.2 IT Service Support Management

The university has constituted an IT grievance redressal committee to look after complaints or grievances of users/parents/employees/alumnae. Suitable action is taken and the user is notified regarding the same and steps are taken to avoid reoccurrence of such complaints.

3.3 Computer Lab Policy

(a) Scan before using a pen/external drive by the students and staff.
(b) No eating OR drinking in the lab.
(c) Files should be saved to disk or to the folder called "Share Folder" and not on the hard drive.
(d) Internet use is a privilege. Do not visit "chat rooms" or sites and unwanted software not specifically authorized by the instructor.
(e) Do not share the internet or file server user name or password with anyone.
(f) Games of any kind, unless authorized by the instructor, are PROHIBITED!
(g) When the work is finished, unless otherwise instructed by the Teacher, QUIT all the programs and put your computer in the Hibernate mode.
(h) Before leaving the Computer lab, PLEASE CLEAN UP THE WORK AREA, put scrap paper in the paper recycling box and arrange the chairs back under tables.

(i) Copying software and/or using pirated software are ILLEGAL AND PROHIBITED.
(j) Do not abuse the hardware. If a problem is encountered with hardware or software, tell your teacher. The teacher will contact the Computer Lab Assistant.
(k) Maintain silence in the computer lab.
Staff person or Lab Assistant MUST BE in the computer lab during the class.

3.4 Meta Campus and Mail Policy

The University maintains two categories of accounts, i.e. Member and student accounts.

3.4.1 Definitions

Definitions in these guidelines are the same as those used in the IT User Account Management Policy.

3.4.2 Member Accounts Management Processes

(a) Member accounts may be one of two types: Teaching or Non-Teaching.
(b) To hold a Member account, an account holder must:
   i. be a paid staff member of the university or one of its subsidiaries;
   ii. hold an honorary academic appointment with the university.
(c) Such accounts are issued for the period of appointment only and as such the account should be used for staff purposes only.
(d) Associate accounts apply to individuals who are granted access to the university IT facilities by virtue of an affiliation with the university or one of its subsidiaries. Recognized affiliations are:
   i. contractors and consultants providing services to the university or one of its subsidiaries;
   ii. visiting academics of the university, other than those holding an honorary academic appointment as in an honorary or visiting fellow;
   iii. members of the University Academic Council or Board of management
(e) The management processes for these are detailed below for:
   i. University staff accounts
   ii. Subsidiary staff accounts

3.4.3 Creation of a new account

(a) For creation of an account, the Registrar officeprovides the details of the member.
(b) The Administrator will create the member account as per the details provided by the HR System.
(c) On the successful creation of account, the Member will be provided a user name and password to access the mail.
(d) Using the credentials the Member has access to webmail.iisuniv.ac.in.

3.4.4 Automatic Account Closure & Reactivation

(a) The closure of university staff accounts' is managed automatically based on appointment details maintained in the HR System. As a consequence, university staff accounts will now automatically close when an account holder's appointment with the university ceases.

(b) For the purpose of managing the official closure of an account, an appointment is deemed to have ended:
   i. After the end date of a permanent or limited term appointment,
   ii. After the last paid date for any other appointment types
(c) Accounts held by University Council award recipients, i.e., Emeritus Professors and Fellows; remain active until the university is advised that the account is no longer required.
(d) Account holders who wish to be contactable on their account following its closure should ensure that they record an automatic reply or forwarding prior to the closure of their account. The automatic reply/forward will continue to operate until the account is deleted.
(e) Closed user accounts are removed from the University Contact Directory within 24 hours of the accounts closure.

3.4.5 Roles & Responsibilities

(a) All the Account holders must agree the agreement of:
   i. Mail service provider
   ii. The University
(b) Member should:
   i. not use the account for any illegal or un-trusted means
   ii. obey university rules and IT policy

If any illegal action or misuse found, the Member shall be responsible for the same.

3.4.6 Student Accounts Management Processes

(a) To hold a Student account, an account holder must:
   i. Regular/Research/ex-student of the university
   ii. Must enroll with the university
(b) Such accounts are issued for life-long and after completion of degree the accounts is automatically transferred as alumni.

3.4.7 Creation of a new account

(a) For creation of an account, the Admission System provides the details of the student.
(b) The Administrator/Admission System will create the student account as per the details provided.
(c) On successful creation of the account, the student will be provided a user name and password to access the mail.
(d) Using the credentials, the student has access to webmail.iisniv.ac.in.

3.4.8 Automatic account closure & reactivation

(a) Closure of an account means the account is frozen, i.e. the password is revoked, until the individual case or misconduct (whichever the case may be) is resolved.
(b) Closed user accounts are removed from the University Contact Directory within 24 hours of the accounts closure.

3.5 File Server User Account

3.5.1 Applicant's Form Details:

All user accounts are uniquely identified by a user name, where the user name may be up to 8 characters. The user name is issued for the duration of your affiliation with the university. The facility and students does not exist to change a user name however in the case of a legal name change where extraordinary circumstances justify a user name change, an Account Holder may be issued a new account, after an application is made in writing and accepted by the authorized person.

3.5.2 User Account Creation:

There are two types of user accounts: student and faculty.
At the time of user creation following is used:

- Student University Enrolment Number for students (Undergraduate (UG), Postgraduate (PG) and Research scholar)
- Faculty Employee number for College Faculty.

3.5.3 User Account Policy:

A User Account Policy dictates the various measures and limitations that are enforced on the user account, in use by university staff and students, for instance, Password Policy, Account Lock Policy, etc.

3.5.4 Password Policy:

All university staff and student user accounts are subjected to the password policy stipulated below:

- Number of day(s) after which a password must be changed: 180
- Number of day(s) before a password may be changed: 1
- Minimum number of characters in a password: 6

For security concerns, everyone is encouraged to change passwords as often as possible.

3.5.5 Password Expiry Reminder

By default, when a user login to a Windows XP/2000 workstation, the user shall be reminded when the password is about to expire in 14 days or less. This will help users to abstain the last minute rush and change password before the expiry date.

3.5.6 User Group Policy:

Based on the nature of the user, the groups are classified as follows:

- Administrative User
- Local User

Suitable user policy is applicable to each group.

3.5.7 Internet Server User Account

All user accounts are uniquely identified by a user name, where the user name may be up to 8 alpha characters. The Employee No./University Enrollment No. details provided on this application form are used to generate the user name. The user name is issued for the duration of your affiliation with the university. The facility and students does not exist to change a user name however in the case of a legal name change where extraordinary circumstances

justify a user name change, an Account Holder may be issued a new account, after an application is made in writing and accepted by the authorized person.

3.6 Web Content Publishing

Any Web document concerning The University and/or its units need to follow this policy and the Web Standards supplement and should be in compliance within a ten days time after any change.

3.6.1 Accessibility

The University web sites must strive to adhere to the Web Content Accessibility Guidelines of the World Wide Web Consortium. These guidelines are required for all web sites of the University, regardless of any written exception approvals of other restrictions in the Web Standards and Guidelines.

3.6.2 Redundancy

Do not repeat static information maintained elsewhere by the University. Redundant information, especially different published versions, is confusing to our audience and may result in severe consequences if incorrect information is posted.

3.6.3 Content Validity

(a) The University controlled sites must be registered under the ***iisuniv.ac.in***.
(b) Individual units at the University are responsible for the content on all of their Web pages.
(c) Content must be up-to-date and follow all sections of this policy and its supplements, as well as national laws and codes.
(d) The verbiage surrounding links to Web pages outside of the University structure cannot be written in such a form that implies endorsement, sponsorship, or other gains.
(e) The Web Administrator has the right to remove the link from all University Web pages to any units that do not follow this policy or its supplements (exceptions are those units that have separate web administrator)
(f) No official unit may go outside the University Web structure and represent itself on another domain without written approval from the Director/ Vice chancellor.
(g) Visible credits such as "Site powered by..." or "Site created by..." are prohibited.

3.6.4 Copyright

(a) The University has copyrights for its all Web pages.
(b) Publishers from the University side must have permission from any copyright holder to use text, photos, graphics, sounds, or movies to which The University does not hold copyrights.

3.6.5 Style

Official University style guidelines must be followed on all Web sites. These guidelines are outlined and detailed in the University Style Guide, which is maintained by the Web Office. Web-specific styles, including, but not limited to, templates, headers, footers, navigation elements, specific required tags, and other required information are outlined in the Web Standards Guide, a supplement document to this Policy, and must be followed at all times.

Chapter 4

4. IT Security Policy

4.1 Objective of IT Security Policy

The purpose of this policy is to outline the acceptable use guidelines for IT equipment and services at the University. The objective of this policy is to promote the University's established culture of openness, trust and integrity. These are general guidelines on what can be done, and what should not be done, on the University ICT Infrastructure in order to protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems.

4.2 Information Security

This policy outlines the provisions made by the University for the use of various IT services by the users, as under-mentioned:

(a) Users do not have a personal privacy right to any matter created, received, stored in or sent from the "IISUNIV IT INFRASTUCTURE". The management may, at any time and without prior notice, screen and review emails and other online content of users in order to ensure appropriate use of the IT infrastructure at the University.

(b) Users should be aware that, during the performance of their duties, network and systems administrators observe the contents of certain data, on storage devices and in transit, to ensure proper functioning of the University's IT facilities. During these processes the contents of users may be accessed, if required.

(c) The University has a legal right to capture and inspect any data stored or transmitted on the University's IT facilities/solutions (regardless of data ownership), while investigating system problems or potential security violations, and to prevent, detect or minimize unacceptable behavior on that facility. This includes maintaining system security and integrity including the management of unsolicited mail, virus protection and protection against any other destructive activities by user.

(d) Users must request a username and password from Web office/Network office in order to access various IT facilities. Users must consider their username and password as private information and should not share the same with any other person. User must change the password provided by Web office/Network office at the earliest.

(e) Once a user logs into any "IT based solution" using her/his username and password on a computer or other device, he/she should not leave the session with IT service/facility open or unattended. The user should log out from that IT based solution before leaving the device unattended.

(f) All users have individual user accounts through which they get personal space on the server hard disk. This is advantageous as the users can store their data at a common place and can access the same from anywhere across the network in the university.

(g) Any activity of destructive nature for information/data on the computer network, like virus spreading (download/upload) on network and spamming is monitored and stopped using licensed Symantec and other technologies.

4.3 Network Security

(a) All servers comply with the minimum server security standards.

(b) Unauthorized access to university data closets is strictly prohibited. In this regard, Subnetting of the entire IISUNIV network is done; wherein different network accounts are created for specialized type of work like administration, accounts, examination, office, various computer laboratories. No unauthorized person outside the subnet can access the subnet. Thus, by providing passwords to these subnets, the network is secured.
(c) Mac filtering is also done.
(d) The whole network is Firewall protected which ensures foolproof security of the network.
(e) Unauthorized access to University networking equipment (routers, switches, hubs, etc.) is not permitted. This includes any port scanning or attempts to access ssh, snmp or otherwise gain access to University equipment.
(f) The University's external Internet firewall policy denies all external Internet traffic to the University's network unless explicitly permitted. Access and service restrictions are enforced by IP address and/or port number. Proxy services are used in conjunction with the firewall to restrict usage to authenticated individuals.
(g) The University offers Internet services to all the systems. To ensure further security these systems are protected by access control software, host-based firewalls, anti-virus server software and filtering, etc.

4.4 Proxy Authentication Policy

4.4.1 Purpose of Policy:

- To ensure that only authorised users can use the Internet facilities, the university has a policy for Web authentication that requires users of the university IT facilities, when browsing the Web, to authenticate themselves via their user name and password.
- The University is committed to the appropriate use of IT & its services in support of its teaching, research, administrative and service functions. This policy is an adjunct to the University's IT Acceptable Use Policy which defines the admissible behaviour expected of users and intending users of the facilities, including the Internet. The university requires users to accept the IT policies and the requirements governing the use of IT facilities as a condition of their use.

4.4.2 Application & Scope:

- This policy represents the university institutional position and takes precedence over other relevant policies which may be developed at a local level.
- Web proxy authentication applies to all users of the university IT facilities except where an exemption has been granted by the IT Officer.
- All users should be aware of the policy, their responsibilities and legal obligations. All users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4.4.3 Proxy Authentication:

- All computers connected to the university network, either via direct connection or wifi connection will have to be authenticated to the Web proxy server to access non-university Websites.
- The University supplied user account is used to authenticate to the Web proxy server.

- On rare occasions the university may give permission for an exemption to this policy but only where the exemption applies for technical reasons. Requests for an exemption must be made in writing to the IT Officer.

Chapter 5

5. Risk Management Policy

5.1. Objective of Risk Management Policy

The risk management is the part of the university's internal control and governance arrangements. The Risk Management policy explains the university's underlying approach to IT risk management and gives key aspects of the risk management process. It identifies the main reporting procedures, and describes the process for the Committee members to evaluate the effectiveness of the university's internal control procedures.

The university adopts risk management measures for the following reasons:

- Effective risk management is a good practice and improves the way the university is run.
- Regular concern of risks helps the HODs (Heads of the departments) to avoid troubles and make effective planning.
- An understanding of the risk areas is essential in developing university strategies and plans.
- Regular reporting of risk enables the Vice-Chancellor / Committee to make appropriate financial or other provisions, wherever needed.

5.2. Approach followed

The University has the following approach to Risk Management:

- Identification of the key IT risks that may obstruct the success objectives.
- A Committee is constituted for managing the risks.
- Assessment of the significance of each type of risk based on their probability and impact. The relationship between different types of risks is identified, so that they can be effectively prioritized.
- Once risks are identified, the concern should be to reduce their probability and impact.
- Ensuring the in-house control system helps to control the risk.
- Regular review of risks avoids troubles.

Chapter 6

6. IT Equipment Maintenance Policy

6.1. Software Assets Management

(a) IT facilities procured/developed with various funds remain the property of the university and are treated as university owned IT facilities. Users cannot duplicate any licensed software or related documentation for use either on university premises or elsewhere unless expressly authorized to do so under the prevailing software agreement.
(b) External parties are not given licensed or copyrighted software.
(c) Users use software on local area networks, servers or on multiple machines only in accordance with the prevailing software agreement.
(d) The university maintains a stock record of all purchased software.

6.2. Open Source Resources

(a) The term "open source" relates to the license conditions under which open source software is made available. The University promotes such open source resources.
(b) The advantage of using open source software is that the university does not become "locked into" any proprietary software platform, i.e., the freedom of choice of using different software is maintained.
(c) The university actively encourages the exploration of open source software solutions in all areas of application. The university staff members who are involved in software development are encouraged to use software which is available under Open Source license terms.
(d) The university also ensures that it imposes no requirement or expectation on students in any discipline that would mandate them to make use of proprietary software involving cost, where there are comparable open source packages available.

6.3. Green Computing

Green computing is the practice of using computing resources efficiently to save energy. The university is committed towards conservation and improvement of the environment by minimizing the impact arising from university activities. The university focuses on better power management, printing and resource use behaviors. In this regard, the university encourages the staff to save power, money and the environment through better management of their departmental computing resources, ensuring optimum use and best output.

Few steps taken in this regard are:

- Publishing the best practices favoring energy saving on the university Website to make everybody aware regarding this initiative
- Environment friendly green infrastructure and services, requiring reduced electricity consumption
- Following the 'reuse, refurbish, recycle' policy
- Other initiatives like reducing the overall "on" time of the system as a whole, reducing the overall "on" time of the monitor in particular, going for emails rather than print outs i.e. go 'paperless', using power saver mode/sleep mode/hibernate

mode, using software/hardware with energy star label, etc. are a few such strategies adopted by the university.

Registrar
IIS (deemed to be University)
Mansarovar, Jaipur-302020