VEER NARMAD SOUTH GUJARAT UNIVERSITY
University Campus, Udhna-Magdalla Road, SURAT - 395 007, Gujarat, India.
વીર નર્મદ દક્ષિણ ગુજરાત યુનિવર્સિટી
યુનિવર્સિટી કેમ્પસ, ઉધના-મગદલ્લા રોડ, સુરત - ૩૯૫ ૦૦૭, ગુજરાત, ભારત.
Telegram : VNSGU, Telephone : +91 - 261 - 2227141 to 2227146, Fax : +91 - 261 - 2227312
E-mail : info@vnsgu.ac.in, Website : www.vnsgu.ac.in
Veer Narmad South Gujarat University, Surat

MINUTES

Meeting of Internal Quality Assurance Cell (IQAC) was held on 03/03/2016, 2:00 pm at Room No. 205, Vahivati Bhavan, VNSGU Campus. Following members were present in the said meeting.

Sr. No.	Name		
1.	Dr. Dakshesh Thakar,	Honble VC	Present
2.	Dr. A. V. Dhaduk,	I/C Registrar	Present
3.	Dr. Apurva Desai	Prof. & Head, Director, IQAC	Present
4.	Dr. M. N. Gayakwad (on behalf of Dr. Parvez Abbasi)	Prof. & Head, (Member)	Present
5.	Dr. Srinivas Rao	Prof. & Head, (Member)	Present
6.	Dr. Rakesh N. Desai	Prof. & Head, (Member)	Absent
7.	Dr. R. D. Patel	Prof. & Head, (Member)	Present
8.	Dr. Kiran Pandya	Prof. & Head, (Member)	Present
9.	Dr. Renuka Garg	Prof. & Head, (Member)	Present
10.	Dr. Mohini Gadia	Prof. & Head, (Member)	Absent
11.	Dr. K. C. Poria	Prof. & Head, (Member)	Present
12.	Dr. V. D. Naik	Principal, (Member)	Absent
13.	Shri J. M. Dhimar	Asso. Professor	Present
14.	Dr. Gaurang Rami	Professor	Absent
15.	Shri Chandrakant Jariwala	President, (Member)	Present
16.	Shri Kamlesh Yagnik	Member	Absent
17.	Shri H. D. Vaghela	I/C Deputy Registrar	Present

Dr. Apurva Desai, Director, IQAC welcomed all members and gave details of actions taken on the decisions made in the earlier meetings.

After thorough discussion, following decisions were taken unanimously by IQAC.

1. To approve the minutes of meeting of IQAC held on 02/11/2015.
   It was resolved to approve the minutes of meeting of IQAC held on 02/11/2015.

2. To discuss Annual Quality Assurance Reports of the University for the year 2014-15.

Resolved to approve Annual Quality Assurance Reports of the University for the year 2014-15 with necessary modification.

3. To discuss Self Study Report (SSR) of the University. (advanced soft copy of the SSR has been already send on members email id, and the hard copy will be provided at the time of meeting).

Dr. Apurva Desai presented information about the process of preparing SSR. He acknowledged services of all the people who were involved in the preparation of SSR. He mentioned that total 81 meeting took place in the process, and also briefed the report to the members of IQAC. IQAC members made some minor suggestions. After discussion on the report, IQAC approved the SSR with suggested minor modification and also suggested to put report before syndicate. IQAC also agreed to submit SSR to KCG for AAA.

4. To approve the guidelines of the "Earn while Learn" scheme for students of the University.

Item was withdrawn.

5. To discuss preparation of question bank.

It was resolved to make past year papers available to the students.

6. To discuss category wise enrollment data of the University for Academic Year 2011-12 to 2014-15.

After thorough discussion, IQAC analysed and noted that number of tribal students and number of tribal girls student have increased. It is further decided to encourage tribal students to get admission in various progrmmes offered by the university. Further, it was noticed by IQAC that PG Programme of university get more applications compare to UG programme per seat.

7. To discuss funds allocation for research to faculties of Colleges and SFI institutes affiliated with the university.

IT was resolved to organize Seminar/ Workshop for Affiliated College to provide guidelines to take benefit of schemes of State and National funding agencies and also suggest SFI institute/colleges to make some budgetary provision for research for faculties from their self-finance fund.

8. Academic audit of various programs by concern board of studies to analyse result of last examination.

IQAC noted and analyzed the results of various examinations and resolved to refer them to the concern BOS/faculty for appropriate action.

It was further resolved to request all the faculties teachers doing project/ consultancy work to submit their project report in the library.

9. With the permission of chairman Dr. Apurva Desai put various IT Policies for Discussion.

It was resolved to approve various IT policies (Network Policy, Policy on format of User ID, Green Computing Policy, Software Assessment Management Policy, and IT Service Policy) of the University with suggested modification. (Annexure-1)

No. IQAC/3712/2016

Dt. 15/03/2016

Director, IQAC

Annexure - 1

VNSGU IT Service Management

1. Purpose:

VNSGU IT's Service Management policy ensures IT service delivery is consistently applied across VNSGU as measured against agreed upon quality standards.

2. Scope:

This is a Policy that applies to all functional university departments and administrative offices within VNSGU.

3. Policy:

All departments that use information technology (IT) shall be responsible for:

3.1 **Implementation:** Implementing the current IT policies.

3.2 **Maintenance**: Maintaining the functionality of the IT systems within their area.

3.3 **Training and awareness:** Facilitating training and awareness of IT policies.

3.3 **Security**: Maintaining the security of the IT systems and the network to which they are connected.

3.4 **Prevention of unauthorized access** : Preventing unauthorized access to university information, personal files and e-mail.

4. Plan of recovery : Creating and maintaining a plan for recovery of mission critical data and systems if loss is sustained.

4.1 **Development and Implementation**

Each Department and administrative office shall adopt policies related to the use of its IT resources. Such policies shall be consistent with the General Policy on the Use of Information Technology and all other university rules and policies, and shall include at minimum the following components:

(1) These policies should require to identify the persons responsible for each kind of resource, only authorized user should use the resources. Where appropriate, the policy should cover issues of shared access, resource limitations, and personal use;
(2) Employee should not use IT infrastructure like telephones, computers, tablets, pads and other IT resources for personal use.

5. Maintenance

Each information technology system at the VNSGU is intended to serve some function or set of functions. The System manager / System engineer will ensure that the IT systems in the unit continue to serve their functions with an appropriate degree of reliability.

6. Training and awareness

As and when required the system manager / Head of the department may arrange proper training to their employees and encourage them to use IT policies. They should also run some awareness programmes so employee will use and implement IT management policies.

7. Security

System manager and Network Administrator(s) are responsible for establishing, communicating and enforcing unit level practices and procedures that promote security. The following areas should be covered:

7.1. Physical security;
7.2 Protection of information, which includes periodic backup and offsite rotation of mission critical systems, applications, and data files;
7.3 Prevention of unauthorized access;
7.4 Detection of security breaches;
7.5 Procedures for reporting security breaches to Registrar or appropriate authority;
7.6 Account auditing which includes the removal of accounts no longer authorized access to the university's information technology resources.

8. Prevention of unauthorized access

System manager / Network Administrator(s) are responsible for department or office level security and procedures that minimize the possibilities of unauthorized access to university or personal files.

(1) Every user should have prescribed level of access to the network.
(2) Even Network Administrator and technical staff should not access the personal file or data of any user.
(3) Network Administrator or technical staff should have full authority to investigate any misconduct.

9. Plan of recovery

Network Administrator should take back up of all critical data on the network so whenever required they can restore system if loss is sustained.

10. System Users' Responsibilities

System Users' Responsibilities Consistent with the VNSGU General Policy on the Use of Information Technology, this policy does not relieve ordinary users of personal computers or systems of the responsibility to maintain and protect the integrity and security of information technology resources. If a computer is connected to the network, the user is responsible for ensuring that the computer is not used to compromise the security of the network. If the computer contains University information resources, the user is responsible for data integrity, data backup, physical security of the machine, and for protecting the system from computer viruses and other attacks.

Risk management Policy

Risk Management

Risk management refers to the practice of identifying potential risks in advance, analysing them and taking precautionary steps to reduce/curb the risk.

VNSGU has developed its Risk Management Policy to formalise its commitment to incorporating the principles of risk management into all aspects of the University.

1. Purpose

1.1 Purpose of the risk management police is :

- Support effective decision-making that is guided by the University's Mission and Vision;
- Ensure a consistent and effective approach to risk management;
- Formalise its commitment to the principles of risk management and incorporating these into all areas of the University;
- Align the University's planning, quality and risk management systems, and their integration into all areas of the University's operations; and
- Ensure robust academic practices effectively manage risk while allowing innovation and development.

2. Scope

2.1 Risk management is incorporated into all areas of the University.

2.2 Risk management is the responsibility of all staff and all areas of the University.

2.3 Critical incident management and work, health and safety risks are covered by specific University policies and procedures.

3. Overview

3.1 The University is committed to excellence and continual improvement, and will continue to encourage innovation whilst maintaining a low-risk profile. Staff are encouraged to adopt a positive approach to risk management, which further strengthens the risk-aware culture (as opposed to a risk-averse culture) of the University.

3.2 Risk management is incorporated into the strategic and operational planning and quality processes at all levels within the University in order to minimise the impact of risk.

3.3 Opportunities and risks are identified and are proactively assessed and monitored by staff on an ongoing basis.

3.4 The University's approach to risk management, including the Risk Management Model and Principles, is aligned with Australian and New Zealand Standard AS/NZS 31000:2009 (*Risk Management Principles and Guidelines*).

4. Risk Management Model

Risk Management Model consists of the following steps:

- **Identify:** Identify the risk events that may prevent or delay the achievement of the University's strategic goals and objectives.
- **Analyse:** Outline the causes, impacts and existing treatments in order to assess the consequence and likelihood of the risk and determine the risk rating.
- **Treat:** Implement both existing and future treatments in order to prevent and/or mitigate the risk.
- **Monitor:** Continually monitor and evaluate the risks and treatments in order to maintain the effectiveness and appropriateness of the University's risk management.
- **Report:** Provide regular reports and updates in order to assure the University and key stakeholders that the risks are being appropriately managed and treated.

5. Roles and Responsibilities

5.1 The Senate and Audit and Risk Committee (sub-Committee of Senate) are responsible for reviewing the risk management practices of the University.

5.2 The Planning, Quality and Risk Committee will be responsible for overseeing the ongoing development, implementation, review and improvement of the University's Risk Management Model. This includes the reporting of significant University-wide risks to the Vice-Chancellor and Audit and Risk Committee as part of the University's governance processes.

5.3 The Members of the Senior Executive and Members of Executive will be responsible for:

- Supporting the ongoing implementation of risk management in all areas of the University's operations;
- The identification, analysis, treatment, monitoring and evaluation, and reporting of significant risks in their relevant Portfolios and Organisational Units;
- Ensuring that staff understand their responsibilities with respect to risk management; and

- Fostering a positive risk-aware culture within their area of responsibility.

5.4 The Risk management committee will coordinate, facilitate and periodically review the University's *Risk Management Policy* and supporting documentation.

5.5 Head of the department and administrative office will ensure that staff within their areas understand their responsibilities and assist in fostering a risk-aware culture. Regular training and assistance will be provided to relevant staff to assist with risk management.

5.6 All staff and students have a significant role in the management of risk within their area of influence. Staff are responsible for adhering to the University's *Risk Management Policy,Risk Management Procedure* and any related documentation.

VNSGU Policy on format of User ID

1. Introduction:
VEER NARMAD SOUTH GUJARAT UNIVERSITY (VNSGU) has a network providing a host of services over the Internet. One of the critical services being provided is the Internet service to its officers, office bearers, employees, and students. VNSGU is in the process of rationalizing the User Login ID's and authentication offered to its users. The present Version 1.0 of the "VNSGU Policy on USER ID" is a step in that direction.

2. Applicability: This policy is applicable to all the users of the VNSGU Internet services.

3. User ID Policy: The major focus is to assign an ID to the users ensure the uniqueness and simplicity for all the VNSGU users. The users of VNSGU will be assigned 3 groups as follows:

1. Admin
2. Staff
3. Students

The User ID for all the employees (Admin, Teaching, Non-Teaching Staff etc.) will be assigned the same user id using VNSGU E-Mail Address policy.

For assigning User ID to the students of VNSGU, the following nomenclature shall be used:

- Department ID - 3 Characters
- Course ID - 2 Characters
- Year of Admission - 2 Characters
- Sr_No - 3 Characters

Example given below to illustrate the procedure that would be adopted in allocating the User ID:

3.1. Sachin Ramesh Tendulkar (Student of MCA Regular Course – Department of Computer Science)

Name of Student: Sachin Ramesh Tendulkar
Name of College: Dept. of Computer Science
College Code: DCS
Year of Admission: 2015
User ID allotted here would be:

dcs0115001 (dcs-Dept. code, 01-Course Code for MCA Regular, 15-Admission Year, 001-Sr. No.)

4. Official User ID's for different Govt. Offices: Some conventions have to be followed as shown below.

Designation	e-mail id
Vice Chancellor	vc
Pro Vice Chancellor	pvc
Registrar	registrar
Dean CDC	deancdc
IQAC Director	directoriqac
Controller of Examination	examcontroller
Chief Account Office	cao
Deputy Registrar (UGC)	dr_ugc
Deputy Registrar (Academic)	dr_academic
Deputy Registrar (General)	dr_general
Assistant Registrar (UGC)	ar_ugc
Assistant Registrar (Academic)	ar_academic
Assistant Registrar (general)	ar_general
Librarian	librarian
Estate Engineer	engineer
Director, Youth Welfare	director_youth
NSS Coordinator	nss
Dean, Faculty of Science	dean_science
Dean, Faculty of Commerce	dean_commerce
Dean, Faculty of Arts	dean_arts
Dean, Faculty of Education	dean_education
Dean, Faculty of Law	dean_law
Dean, Faculty of Medicine	dean_medicine
Dean, Faculty of Engineering including Technology	dean_enginnering
Dean, Faculty of Rural Studies	dean_ruralstudy
Dean, Faculty of Computer Science and Information Technology	dean_computer
Dean, Faculty of Homeopathy	dean_homeapathy
Dean, Faculty of Architecture	dean_architecture
Dean, Faculty of Management	dean_management
HoD of Department	hod_{department name}
OS of a section	os_{section name}
Principal of College	prin_{college code}
Teacher of College	Initial{college code}
PA to VC	pa_vc
PA to PVC	pa_pvc
PA to Registrar	pa_registrar

These ID's are official positions and will remain permanent. These ID's may be mapped to the actual person who is holding the present position. When a new person comes to the same position on transfer, the mapping will be changed to new person id.

Department	Department Abbreviation
Aquatic Biology	dab
Biosciences	dbs
Bio Technology	dbt
Chemistry	dch
Commerce	dco
Comparative Literature	dcll
Computer Science	dsc
Economics	dec
Education	ded
English	den
Management	dmg
Gujarati	dgu
Human Resource Development	dhr
M.Sc. (IT)	dit
Law	dlw
Library Science	dls
Mathematics	dmt
Physics	dph
Public Administration	dpa
Rural Studies	drs
Architecture	dar
Fine Arts and Interior Designing	dfa
Journalism	djr
Sociology	dso
Statistics	dst
Usic	usic
Examination	exam
Computer Pool	compool
General Section	general
Dispatch Section	dispatch
Senate and Syndicate	senate
Academic Section	academic
Post Graduate Section	Pg
Account Section	account
Estate Section	estate
Physical Education Section	phyedu
NSS Section	nss
Legal Cell	legal
SC/ST Cell	scst
Statistical Cell	statcell
RTI Cell	rti
University Health Centre	health
UGC Section	ugc

5. The following policy will be adopted for the various Internet Services for the categories of groups/users of VNSGU:

Policy Description	All	Admin	Staff	Students
Social Media Applications	Block	--	--	--
Web browsing	Allow			
E-Mail Service	Allow			
Audio Video download (Youtube etc.)	--	Allow	Allow	Deny
Porn Sites	BLOCK			
Chat, Messenger Apps.	Block			

6. No quota is currently defined to be applied to any user/group of VNSGU as of now.

7. Any illegal activity performed by any user of VNSGU over this Internet facility, will face legal prosecution as the law applicable thereof, and also would be liable to punishment as per VNSGU rules.

8. Access to the Internet through WiFi Access Point will be through secured protocols only. For connection password to Access points, user should contact the Administrator.

NETWORK POLICY

1.0 Overview

The University wishes to provide a secure network infrastructure in order to protect the integrity of data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

2.0 Purpose

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the University's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

3.0 Scope

This policy covers all IT systems and devices that comprise the University network or that are otherwise controlled by the University.

4.0 Policy

4.1 Network Device Passwords

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords. Refer to Password Policy for details.

4.1.1 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, system will lock a user's account after 3 unsuccessful logins. In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.1.2 Change Requirements

Passwords must be changed according to the University's Password Policy.

4.2 Networking Hardware

Networking hardware, such as routers, switches, hubs, bridges, and access points, should be implemented in a consistent manner. If possible for the application, switches are preferred over hubs.

4.3 Network Servers

Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. Domain security policy supported by the native operating system should be configured and enforced to all the users and computers belonging to the Domain.

4.4 Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The University neither requires nor prohibits the use of IDS or IPS systems. The decision to use IDS/IPS systems is left to the discretion of the IT Manager.

4.5 Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the University's network security. Security testing can be provided by IT Staff members, but is often more effective when performed by a third party with no connection to the University's day-to-day Information Technology activities.

4.6 Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the University's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the University must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
- The University should consider the use of data wiping technology. Simply reformatting a drive or erasing data does not make the data unrecoverable. If the University chooses to use data wiping technology, it should use the most secure commercially-available methods for data wiping if possible. Alternatively, destroying the device's data storage mechanism (such as its hard drive or solid state memory) will make the data unrecoverable.

4.7 Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network

ensures that the University's IT Staff has a firm understanding of the network architecture at any given time.

The University encourages network documentation, but does not require it.

4.8 Antivirus/Anti-Malware

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire University. The University provides the following guidelines on the use of antivirus/anti-malware software:

- All University-provided user workstations must have antivirus/anti-malwaresoftware installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

4.9 Software Use Policy

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The University provides the following requirements for the use of software applications:

- Only legally licensed software, authorized by Management, may be used. Licenses for the University's software must be stored in a secure location.
- Open source and/or public domain software can only be used with the permission of the IT Manager.
- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that the University uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

4.10 Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple re-boot,an upgrade, or other maintenance. When this occurs, the IT Staff should make every effort to perform the tasks at times when they will have the least impact on network users.

4.11 Change Management

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT Staff should make a reasonable effort to document hardware and/or configuration changes to network devices.

4.12 Suspected Security Incidents

When a security incident is suspected that may impact a network device, the IT Staff should refer to the University's Incident Response Policy for guidance.

4.13 Redundancy

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. The University wishes to provide the IT Manager with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed.

4.14 Manufacturer Support Contracts

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the University should consider purchasing a maintenance plan, support agreement, or software subscription that will allow the University to receive updates to the software and/or firmware for a specified period of time.

4.15 Security Policy Compliance

It is the University's intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind the University requires the following:

4.15.1 Information Security Officer

An employee must be designated as a manager for the University's security program. He or she will be responsible for the University's compliance with this security policy and any applicable security regulations. This employee must be responsible for A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on the University's information security program (as detailed below), D) any ongoing testing or analysis of the University's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

4.15.2 Security Training

A training program must be implemented that will detail the University's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed annually.

4.15.3 Security Policy Review

The University's security policies should be reviewed annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to the University's security policies. As part of this evaluation the University should review:

- Any applicable regulations for changes that would affect the University's compliance or the effectiveness of any deployed security controls.

- If the University's deployed security controls are still capable of performing their intended functions.

- If technology or other changes may have an effect on the University's security strategy.

- If any changes need to be made to accommodate future IT security needs.

4.16 Applicability of Other Policies

This document is part of the University's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of University property (physical or intellectual) are suspected, the University may report such activities to the applicable authorities.

6.0 Definitions

ACL A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Antivirus Software An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Firewall A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Hub A network device that is used to connect multiple devices together on a network.

IDS Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.

IPS Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

NTP Stands for Network Time Protocol. A protocol used to synchronize the clocks on networked devices.

Password A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

RAID Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.

Switch A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.

VLAN Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.

Virus Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

Green Computing Policy

Green computing best practices and policies includes power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines.

1. **Develop a sustainable green computing plan**: Such a plan should include recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment.

2. **Recycle**: Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner. Computers have toxin metals and pollutants that can emit harmful emissions into the environment. Never discard computers in a landfill. Recycle them instead through manufacturer programs

3. **Prefer environmentally friendly products during Purchase decisions**:

- Help institutional purchasers evaluate, compare and select desktop computers, notebooks and monitors based on environmental attributes
- Recognize manufacturer efforts to reduce the environmental impact
- Make a clear, consistent set of performance criteria

4. **Reduce Paper Consumption**: There are many easy, obvious ways to reduce paper consumption: e-mail, electronic archiving, use the "track changes" feature in electronic documents, rather than redline corrections on paper. When you do print out documents, make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

5. **Conserve energy**: Turn off your computer when you know you won't use it for an extended period of time. Turn on power management features during shorter periods of inactivity.

Power management allows monitors and computers to enter low-power states when sitting idle. By simply hitting the keyboard or moving the mouse, the computer or monitors awakens from its low power sleep mode in seconds. Power management tactics can save energy and help protect the environment

6. Including in Education

In educational institutes make Green IT subject a compulsory one rather than an optional one, so that new ideas can be developed by students , based on Green IT and with that innovation in this field that could make products more cheaper and less hazardous and should have the abilities to attract more customers than normal products. By introducing in educational institutions is the only way to invite more project and ideas. Awards, scholarships should be made to increase more and more contribution in this field. Awareness among public is required but what if cheaper healthy products are launched in market definitely people will get attracted to buy them.

Conclusion:

Green computing represents a responsible way to address the issue of global warming. By adopting green computing practices, can contribute positively to environmental stewardship— and protect the environment while also reducing energy and paper costs.

Software Assets Management Policy

Keep one central software repository:

By keeping proof of software licenses at one common place, organization will save time and money by quickly being able to respond to vendor audit requests.

Track license usage/entitlement:

A license entitlement is the number of installs you have of a product. This is important for auditing purposes, as well as to reveal how many unused licenses you have. Once you have this information, you'll be able to reassign licenses from one department, or group, to another based their usage requirements. The best way to manage this is with a **SAM tool**.

Know your product use rights & apply them:

Product use rights dictate how you can use your software licenses and are typically found in your license agreements. It defines your rights for upgrades, downgrades, second use, virtual machine use, multiple versions, etc. These rights can vary from vendor to vendor and from product to product.

Assign users appropriate rights:

If your organization allows employees to install software themselves, it's important that they follow certain installation and reporting processes.

Develop strategic purchasing/renewal requirements:

Checking actual software usage and cross referencing it to headcount provides a more accurate forecast of your purchasing new software or renewal needs.

Conclusion:

ITAM spans across by simplifying IT operations, improving resource productivity, supporting compliance, and asset procurement planning. Simplified, centralized and automated asset management is key to improving your overall IT administration's operational efficiency.