Shri Mata Vaishno Devi University
Network Centre Policies & Guidelines

Network Centre
SMVDU, Katra

INDEX

Appendix

SMVDU Network Centre

Background

Since the University's initial setting up of campus-wide network in 2005, active users of the network facilities have increased many folds and the network-based applications have increased phenomenally. This is a welcome change in the university's academic environment. This has prompted the University administration to rapidly increase the network facilities to all the sections of the university community. Network Centre has been given the responsibility of running the university's Intranet & Internet services.

Network Centre serves as the control point for the Internet facility available in the **Shri Mata Vaishno Devi University**. It covers all Departments, Hostels, Administrative Offices, Medical Aid Centre, Guesthouse, and has even provided the services to faculty residences as well. **SMVD UnivNET** (SMVDU University Network) has been built using Cisco Switches, Network Management System, L3 Switch and Pix Firewalls. Internet services are provided from two Internet Service Providers viz. BSNL. Now, **SMVD UnivNET** has over more than **2000 network connections** across the campus. The essential services provided by the Network Centre includes:-

1. 1 Gbps Internet Link of NMEICT (National Mission on Education through Information & Communication Technology) established for better Internet & virtual classroom facility in future at SMVDU.
2. Central Authentication Mechanism for Internet facility using Network Management System (Internet Gateway).
3. Maintenance of **SMVD UnivNET** connectivity via OFC throughout SMVDU Campus using Cisco Layer 3 Core Switch, over 40 distributions manageable switches, primary & secondary Firewall, etc.
4. Maintenance of Primary & Secondary Domain controller, Biometric Server, NPTEL Server etc.
6. Providing Video Conferencing facility at VC Conference Hall.
7. Maintenance of backup facility.

Need for IT policy

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. While educational institutions are providing access to internet to their faculty, students and staff, they face certain constraints:

- Limited internet bandwidth.
- limited infrastructure like computers, computer laboratories,
- limited financial resources in which faculty, students and staff should be provided with the network facilities, and
- limited technical manpower needed for network management.

On one hand, resources are not easily available for expansion to accommodate the continuous rise in internet needs, on the other hand uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to teaching/learning processes nor governance of the university. At the outset, we need to recognize the problems related to uncontrolled surfing by the users:

- Prolonged or intermittent surfing, affecting quality of work.
- Heavy downloads that lead to choking of available bandwidth.
- Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.
- Confidential information being made public.

With the extensive use of the internet, network performance suffers in three ways:

- when compared to the speed of local area network (LAN), internet traffic over the wide area network (WAN) is a potential bottleneck.
- when users are given free access to the internet, non-critical downloads may clog the traffic, resulting in poor quality of service (QOS) and affecting critical users and applications.
- when computer systems are networked, viruses that get into the LAN,

through intranet/internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users who are on the high speed LAN's trying to access internet resources through a limited bandwidth, definitely create stress on the internet bandwidth available. Every download adds to the traffic on the internet. This adds to costs and after a point, brings down the quality of service.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network. Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe download, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network. They can slow down or even bring the network to a halt. Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, **Network Centre has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.** However, in the absence of clearly defined **IT policy**, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users. As it users are aware, all the educational institutions worldwide have IT policy implemented in their respective institutions.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation. Policies also serve as blueprints that help the institution implement security measures. **Thus, an effective security policy is as necessary to a**

good information security program as a solid foundation to the building. Hence, Shri Mata Vaishno Devi University also is proposing to have its own IT policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, intranet and internet access facilities, collectively called **"Information Technology (IT)"**.

Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this University. While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the information technology, information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of university community to understand how university policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

1. **IT Hardware Installation Policy**
2. **Software Installation And Licensing Policy**
3. **Network (Intranet & Internet) Usage Policy**
4. **E-Mail Account Usage Policy**
5. **Guidelines for running Application Servers/ Services**

It may be noted that university IT policy applies to technology administered by the university centrally or by the individual departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorized resident or non-resident visitors on their own hardware connected to the university network. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the do's and

don’ts detailed in the university IT policy. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the university’s information technology infrastructure, must comply with the guidelines. Certain violations of it policy laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

PURPOSE: Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. To ensure that use of the Internet / Intranet facilities among employees of the SMVDU is consistent with Network Centre policies, all applicable laws, and the individual user's job responsibilities.

.

Software Installation Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

A. **Operating system**

- Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through internet. This is particularly important for all MS windows based computers (both PC and servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.
- University as a policy encourages user community to go for open source software such as Linux, Ubuntu OS and open office to be used on their systems wherever possible in SMVDU Campus.

B. **Antivirus software and its updating**

Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use.

University now go though Open Source Office that can be installed in any PC/Laptop/Server using the following steps:

1. Install the setup file from their respective department wise folder and no need to restart your machine at the end of the installation process.

C. Noncompliance

SMVDU faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons an individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

D. Network centre/MC interface

Network centre upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the MC, if applicable. The individual user wills follow-up the notification to be certain that his/her computer gains necessary compliance.

Network (Intranet & Internet) Usage Policy

Network connectivity provided through the university, referred to hereafter as "the network", through an authenticated network access connection, is governed under the university IT policy. The communication & information services (network centre) are responsible for the ongoing maintenance and support of the network, exclusive of local applications. Problems within the university's network should be reported to network centre.

A. IP address allocation

Any computer (pc/server) that will be connected to the university network, should have an ip address assigned by the network centre. Following a systematic approach, the range of ip addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated ip address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that ip address so that no other person uses that ip address unauthorized from any other location.

B. DHCP and proxy configuration by individual departments / users

Use of any computer at end user location as a dhcp server to connect to more computers through an individual switch/hub and distributing ip addresses (public or private) should strictly be avoided, as it is considered absolute violation of ip address allocation policy of the university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by network centre. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/dhcp configuration. Non-compliance to the ip address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running network services on the servers

Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., http/web server, SMTP server and many

application servers, only after bringing it to the knowledge of the network centre in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the network. Network centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the network's performance. Access to remote networks using a university's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the university network connects. University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at network centre. Impersonation of an authorized user while connecting to the network is in direct violation of this agreement and will result in the termination of the connection.

D. Wireless local area networks

- This policy applies, in its entirety, to school, department, or division wireless local area networks. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with network centre including point of contact information.
- School, departments, or divisions must inform network centre for the use of radio spectrum, prior to implementation of wireless local area networks.
- School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or mac/ip address restrictions. Passwords and data must be encrypted.
- If individual school wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Director, network centre.

E. **Network Access Usage Rule**

1. Any other university employee residing in the campus or any visiting guest who want internet connection should get prior permission for the same from the competent authority.
2. Network centre will be providing internet connection only in case of approval from competent authority.
3. If any university employee, wants to create an email account in the SMVDU should ask for the same by a written application forwarded through proper channel.
4. If network centre will detect any case of hacking, prone or illegal websites viewing, serious and immediate action will be taken.
5. Commercial use - any form of commercial use of the Internet is prohibited.
6. Copyright violations - any use of the Internet that violates copyright laws is prohibited.
7. Harassment - the use of the Internet to harass employees, vendors, customers, and others is prohibited.
8. Political - the use of the Internet for political purposes is prohibited.
9. Aliases - the use of aliases while using the Internet is prohibited. Anonymous messages are not to be sent. Also, the misrepresentation of an employee's job title, job description, or position in the County is prohibited.
10. Misinformation/Confidential Information - the release of untrue, distorted, or confidential information regarding County business is prohibited.
11. Employees who are found in violation of this policy may be subject to the following:
    (a) Internet & Email access may be revoked.
    (b) Access times may be restricted
12. Employees should keep personal logons and passwords confidential and change passwords on a regular basis as instructed by Information.
13. The e-mail system is not to be used to send, receive or download copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

14. The electronic mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job related solicitations.
15. If you receive such Racism, sexism messages, please forward them to the Network Incharge Head or Server Manager or Network Manager. If you send such messages, expect to have your manager notified.
16. Users name are provided for academic research and instruction, electronic mail, Internet access, and for activities related to the mission of SMVDU. Each account represents an allocation of computing resources and as such is monitored by Network administrators for appropriate use. Each User Name is assigned for the sole use of a single user. Sharing of User Names is prohibited. The user for whom the account was created is responsible for the security of the account and all actions associated with its use. An account may be revoked if it is found to have been used for activities that violate any portion of this policy, the owner of the User Name has been found violating any portion of this policy, or the owner of the User Name is no longer enrolled or employed by SMVDU. Activation of an account on an SMVDU host computer constitutes an agreement stating that the user understands and will abide by all IT policies regarding the use of the SMVDU network.
17. Any kind of damage or loss of networking equipments (Ethernet Cable, Modem, Wireless Card, Access Point, Hub, Switch) bore by User whom the Networking Equipment is issued.
18. Any kind of internet connectivity problem at residences must be conveyed in proper format.
19. Any event that is going to be organized in the university campus must be conveyed well before its commencement for the purpose of related services from network centre.
20. The accounts for Internet access have the following bandwidth allocation ratio:-

    Faculty/Guest/Students : 1 Mbps

E. **Preservation of network equipment and accessories**

Routers, switches, fiber optic cabling, utp cabling, connecting inlets to the network, racks, ups, and their batteries that are installed at different locations by the university are the property of the university and are maintained by network centre. Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

i) Removal of network inlet box

ii) Removal of utp cable from the room

iii) Opening the rack and changing the connections of the ports either at jack panel level or switch level

iv) Taking away the ups or batteries from the switch room.

v) Disturbing the existing network infrastructure as a part of renovation of

the location

Network centre will not take any responsibility of getting them rectified and such tampering may result in disconnection of the network to that segment or the individual, until the compliance is met.

G . **Additions to the existing network**

Any addition to the existing network done by school/centre, department or individual user should strictly adhere to the University Network Policy and with prior permission from the competent authority and information to network centre. In this regard, instructions for deployment may be sought from the Network Centre.

Non-compliance to this policy will be treated as direct violation of the university's IT security policy.

SHRI MATA VAISHNO DEVI UNIVERSITY

Sub Post Office, Katra -183230
Ph. # 01991-285535, 285634 Fax : 01991-285573

Network Centre

Application Form for Internet Connectivity / Email for Staff/ Faculty

Name	
Employee Code	
Department/School	
Permanent address	
University Address	
Laptop / System Model & Serial No. (if any) **1. MAC ID of LAN Card** **2. MAC ID of Wi-Fi Card**	
Mobile No.	
Email Id 1. (Preferred University Email ID) **2. (Other Email)**	
Signature	
Recommended & forwarded by **Dean / Directors/ Section Heads**	

For Network Centre use

SMVDU/NC/2015/ Dated :

Username : _____ Password : _____

_ _

Username : _____ Password : _____

Instructions: -

1. Do not share username & password with anyone.
2. Network centre will be providing internet connection only as per recommendations from Deans /Directors / Head of Sections.
3. The user for whom the account was created is responsible for the security of the account and all actions associated with its use.
4. **Stolen passwords:** Often the account owner is the first person to detect unauthorized use of their account. If this occurs, please notify to the Network Centre.
5. Type **ipconfig /all** in command prompt to see the MAC ID of Network Card.
6. Attach one photocopy of your identity card with this form.

SHRI MATA VAISHNO DEVI UNIVERSITY

Sub Post Office, Katra -183230
Ph. # 01991-285535, 285634 Fax : 01991-285573

Network Centre

Application Form for Internet Connectivity through LAN/WIFI / Email for Student

Name		Affix Attested Photo
Enrollment No		
Department/School		
Semester		
Permanent address		
University Hostel Address		
Laptop / System Model & Serial No. (if any) **1. MAC ID of LAN Card** **2. MAC ID of Wi-Fi Card**		
Email Id		
Mobile No.		
Signature		
Recommended & forwarded by Warden		
Recommended & forwarded by Director of School		

Declaration

I _____son/daughter of _____student of SMVDU will use SMVDU Internet for educational and research work only. I hereby abide by the rules and regulations of SMVDU internet policy and will not indulge in activities like hacking/ using proxy servers/ torrent download, etc. I will not share the internet credentials with anyone and will be fully responsible for usage of Internet Account.

Signature: - _____ Date: - _____

For Network Centre use

SMVDU/NC/ / Dated :

Username : _____ Password : _____

Instructions: -

1. Do not share username & password with anyone.
2. Network centre will be providing internet connection only as per recommendations from Deans /Directors / Head of Sections.
3. The user for whom the account was created is responsible for t he security of the account and all actions associated with its use.
4. **Stolen passwords:** Often the account owner is the first person to detect unauthorized use of their account. If this occurs, please notify to the Network Centre.
5. Type **ipconfig /all** in command prompt to see the MAC ID of Network Card.
6. Attach one photocopy of your identity card / photo graph with this form.

SHRI MATA VAISHNO DEVI UNIVERSITY
SUB POST OFFICE, PIN – 182320, J & K,
NETWORK CENTRE

Tell us about any problems you may have experiences with LAN. Your complaint, depending on the nature of the case, you will be contacted shortly.

Internet/LAN Complaint Form

Name of Employee/Student :		Designation/Department :	
Cabin/Room/Qtr No:		Dated	
Hostel/Residence/Academic Block:			
Extension /Mobile No.			

Employee Code /Entry No.:-

Have you checked your LAN Cable (i/o Box) other than your Computer/Laptop? ☐ Yes ☐ No

Please give us the details of your complaint along with suitable time to visit your office/room below:-

Tick Mark the relevant Box

☐	Cable Wire Installation	☐	Internet Login Problem	☐	Server Services Related
☐	LAN I/O BOX Problem	☐	Wi-Fi Problem	☐	Network Printer

* Network Centre may charge for network equipments as per Network Centre Policy.
* Kindly send the complaint form through proper channel.

Signatures of Employee/Student :

Signatures of Dean/Dir/HOD/Section Head/Hostel Caretaker :

I/c Network Centre :

For Official use only

Complaint No.:	**Action Taken:**
Items Installed/Used	
Problem Solved ☐ **YES** ☐ **NO**	**Signature of Employee/Student:** **Dated :**

Recommendation (if any):

Signature of Network Coordinator:

Shri Mata Vaishno Devi University

Network Centre Computer Maintenance Cell

……

Date:

Complaint Form for Desktop/Laptop/Printer

Name of Employee: _____ Designation: _____

Department: _____ Mobile No. and Ext. No. _____

Nature of Complaint (Hardware/Software) _____

Description of Complaint _____

_____

_____

- Please take backup of your data before sending CPU
- Never save your data in C drive/Desktop/My Document

Signature of Employee

Signature of Dean/Dir/HoD/Section Head

I/c Network Center

For Official use only

Complaint No: _____

Action Taken _____

Items Installed/Used _____

Recommendation _____

Signature of Computer Maintenance Coordinator

Signature of Receiver
Name:
Date:

Shri Mata Vaishno Devi University

Network Center Computer Maintenance Cell

.....

Date:

Computer/Laptop Replacement Form

Name of Employee: _____ Designation: _____

Department: _____ Phone No. and Ext. No. _____

Brand/Model No. :_____ Purchase/Issued year_____

Fill Configuration Details:- Status:- Working/ Not-Working

1. RAM _____ ☐
2. Hard Disk _____ ☐ ☐
3. Processor _____ ☐ ☐
4. Moniter (TFT/LCD) _____` ☐ ☐
5. Any other.....

.....

Signature of Employee

Signature of Dean/HoD/Section Head

Maintenance In-Charge, Network Centre

Inspection Report

1. Working/Serviceable/obsolete 2. If serviceable list of items needed to be replaced/repaired

1_____2_____

3_____4_____

5_____

Recommendations/Observation (If any):_____

_____

Maintenance coordinator signature

Dated:

I/c Network Centre

for verification of date of purchase/year and necessary action, please

AR(S&P)

Shri Mata Vaishno Devi University

Network Centre Computer Maintenance Cell

……

Date:

Battery Replacement Form

Name of Employee: _____ Designation: _____

Department: _____ Mobile No. and Ext. No. _____

LAPTOP Model No.(4420s/4410s).....Laptop Issue date/year.....

Battery Model Number (ZP06/PH06/**).....Battery Sr. No (*).....

Last Battery Replaced Date (Required only if you want to replace battery before 2 years).....

Reason for replacement:

1. Back up time: (Mention Battery backup time).....
2. Any other : _____

Signature of Employee

Signature of Dean/Dir/HoD/Section Head

AR(S&P)

S&P office

Under Warranty YES/NO

I/c Network Center

For Official use only

Action Taken Battery Replaced/ Not Replaced Replaced Date:

Battery Sr. No.....

HP Compatible/Original.....

Recommendation _____

Signature of Computer Maintenance Coordinator

Signature of Receiver
Name:
Date:

*For HP Original Battery serial number start with CT and for others start from GH

** Model number is relevant only in case of HP original battery installed in your Laptop

Shri Mata Vaishno Devi University

Network Center Computer Maintenance Cell

.....

Date:

Computer/Laptop Replacement Form

Name of Employee: _____ Designation: _____

Department: _____ Phone No. and Ext. No. _____

Brand/Model No. :_____ Purchase/Issued year_____

Fill Configuration Details:- Status:- Working/ Not-Working

1. RAM _____ ☐
2. Hard Disk _____ ☐ ☐
3. Processor _____ ☐ ☐
4. Moniter (TFT/LCD) _____` ☐ ☐
5. Any other.....

.....

Signature of Employee

Signature of Dean/HoD/Section Head

Maintenance In-Charge, Network Centre

Inspection Report

1. Working/Serviceable/obsolete 2. If serviceable list of items needed to be replaced/repaired

1_____2_____

3_____4_____

5_____

Recommendations/Observation (If any):_____

_____

Maintenance coordinator signature

Dated:

I/c Network Centre

for verification of date of purchase/year and necessary action, please

AR(S&P)

E-waste form for Computers and Peripherals

Name of the Department: | **Date**

Total no of LAPTOP / DESKTOP /SCANNER /PRINTER deposited as e-waste in the past prior to 1st July 2017

1. **LAPTOPs .....**
2. **Desktops.....**
3. **Printers.....**
4. **Scanners.....**

Sr. No.	Description of the Items (LAPTOP / DESKTOP / SCANNER / PRINTER)	Brand Name (HP/Dell /IBM, etc)	Model No.	Configuration of (LAPTOP / DESKTOP)			Year of Purchase	Accessories sent with the items					Identification Number given by the Department	Signature of concerned faculty / Staff/ Lab In-charge
				Processor (Intel /AMD etc) with speed	RAM	HDD		Keyboard Brand with Type (USB / PS2)	Mouse Brand with Type (USB / PS2)	Display Terminal Brand with Type (LCD / LED / CRT)	Display cable (VGA / HDMI)	No. of Power Cables		
1														
2														
3														
4														
5														
6														

Note: 1. Apart from Hardcopy, Softcopy of the e-waste form must be send to icnetwork@smvdu.ac.in

2. All entries need to be filled in each column by the concerned as an example given below:

Desktop Dell optiplex330 Intel i3 2GB 320GB 2007 Dell USB Dell PS2 Dell LED VGA 2 SMVDU/CSE/Ilab/128 Sign

7														
8														
9														
10														
11														
12														

*To add more no of rows kindly download soft copy of e-waste form from network.smvdu.ac.in

Total No of Computers:-_____Total No of Laptops:_____Total No of Printers_____ Total No of Scanners_____

Total No of Keyboards:-_____ Total No. of Mouse:-_____

Head of Department/Section Signature	
Name	
Date	

Forwarded to in-charge network/Chairman e-waste computer committee

Signature of E-waste committee members

Note: 1. Apart from Hardcopy, Softcopy of the e-waste form must be send to icnetwork@smvdu.ac.in

2. All entries need to be filled in each column by the concerned as an example given below:

Desktop Dell optiplex330 Intel i3 2GB 320GB 2007 Dell USB Dell PS2 Dell LED VGA 2 SMVDU/CSE/Ilab/128 Sign

Member1 Member2 Member3:

Note: 1. Apart from Hardcopy, Softcopy of the e-waste form must be send to icnetwork@smvdu.ac.in

2. All entries need to be filled in each column by the concerned as an example given below:

Desktop	Dell	optiplex330	Intel i3	2GB	320GB	2007	Dell USB	Dell PS2	Dell LED	VGA	2	SMVDU/CSE/Ilab/128	Sign

COMPUTER ISSUE FORM OF NETWORK CENTRE STOCK

Name of the Department: | **Date**

Sr. No.	Description of the Items (LAPTOP / DESKTOP / SCANNER / PRINTER)	Brand Name (HP/Dell /IBM, etc)	Model No.	Configuration of (LAPTOP / DESKTOP)			Year of Purchase	Accessories sent with the items					Identification Number given by the Department	Signature of concerned faculty / Staff/ Lab In-charge
				Processor(Intel/AMD etc) with speed	RAM	HDD		Keyboard Brand with Type (USB / PS2)	Mouse Brand with Type (USB / PS2)	Display Terminal Brand with Type (LCD / LED / CRT)	Display cable (VGA / HDMI)	No. of Power Cables		

Issued by Signature		**Received by Signature**	
Name		**Name**	
Date		**Date**	

in-charge network

: