VIDYASAGAR UNIVERSITY

IT Policies, Rules and Regulations

Table of Contents

Introduction:

Vidyasagar University makes available to its community members computing and network resources, including shared information technology resources that use text, voice, images, and video to deliver information. These resources are to be used in a manner consistent with University policy and the IT Act/ law, including this policy, and related policies created by specific departments, programs and offices of the University.

Importance of this IT Policy, Rules and Regulations

The University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure made available by the University on the campus for all its stakeholders.

This policy specifies University-wide strategies and responsibilities for protecting the **Co**nfidentiality, **I**ntegrity, and **A**vailability of the **information assets** that are accessed, created, managed, and/or controlled by the University and its stakeholders.

Information assets addressed by the policy include data, voice, video, images, information systems, computers, Printers, UPS, Thin clients, Mobile, Laptop, Tablets, Projectors, Multimedia A/V devices, Smart Classroom accessories, CCTV Surveillance components, network devices, intellectual property, as well as documents and verbally communicated information.

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, Vidyasagar University initiated, way back in 2004, the establishment of a basic network infrastructure in the academic complex of the university.

However, the IT infrastructure development in the Campus began, in its true sense, over the last 7 years. In consequence to that, not only active users of the network facilities have increased manifold but the web-based applications have increased too. This is a welcome change in the university's academic environment. The University Portal - based student life cycle - management system has been an added feather in the existing IT infrastructure for the entire University Management.

Now, the university has about 2000 network connections covering more than twenty buildings across the campus and 5000 users inside the campus and lacs of users outside the campus.

The Computer Centre is the department that has been given the responsibility of planning, designing, implementation and maintenance of various IT Infrastructure and support services to the whole university's intranet & Internet, WI-FI, CCTV, University management portal, the Smart and Virtual classrooms, support to T-L Process, SWAYAM, Digital initiatives, Digital Signages and BSNL Data and services.

Network Control Unit of the Computer Centre is housing the Firewall security, Proxy, DHCP, DNS, Core Switching devices, WI-FI Control Unit, Surveillance Control Unit, Data Storage Unit and application servers and managing the network of the university, University Management Portal.

The Central Library of the University is at present providing the complete RFID based Automated Library Services. It is maintaining the University website and online services.

University Management portal is being developed under Computer Centre and is being hosted in the cloud for the Complete University and Student Management System.

Vidyasagar University is getting its Internet bandwidth from BSNL. It has got 1 Gbps connectivity under NKN Network of MHRD (NME-ICT) via BSNL.

While educational institutions are providing access to various IT services and facilities to their faculty, students and staff and all other stakeholders, 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
- Limited technical manpower needed for network management.
- ICT unawareness and unacceptability among a group of Staff members.

On one hand, resources are not easily available for expansion to accommodate the continuous rise in user counts, demand for more IT hardware and software, Internet bandwidth ; on the other hand, misuse of IT hardware and Licensed Software, uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes nor governance of the university.

Hence IT Policy / regulations is necessary to be adopted/followed by the stakeholders to secure the complete network from various threats /viruses/hackers etc.

As IT users are aware, all the educational institutions worldwide have IT policies 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.

Hence, Vidyasagar University is proposing its own IT Policies /regulations that work as guidelines for using the university's computing facilities and IT Infrastructure including computer hardware, software, email, web-sites, information resources, intranet and Internet access facilities, collectively called **" Vidyasagar University IT POLICY, Rules and Regulations 1.0"**

This document defines IT policies and guidelines that would be relevant in the context of Vidyasagar University.

Henceforth, 'University IT Policy' shall mean all the IT Policies and Regulations laid down by the University.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the right functions by the users.

Further, due to the dynamic nature of the Information Technology, Information security in general and, therefore, policies/regulations 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.

Purposing IT policy/regulations is to offer a direction and provide information about acceptable actions and prohibited actions or policy violations.

Guidelines are created and provided to help the organisation, departments and individuals who are part of university community to understand how the University IT policy applies to some of the significant areas and to bring conformance with the stated policies.

It may be noted that the 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 authorised resident or non-resident visitors on their own hardware connected to the university network. The University IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university, recognised Associations/Unions, or hostels and guest houses, or residences wherever the network facility is provided by the university.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network shall come under the jurisdiction detailed in the university IT policy.

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure University IT Policy must comply with the Violation of the University IT Policy laid down by the university by any university member may result in disciplinary action against the offender by the university authorities. If the matter involves illegal activity, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

- Students, Research Scholars: UG, PG, M.Phil, Ph.D
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests
- Project Fellows

Authorities:

- ICT& MIS Working Committee
- Hon'ble Vice-Chancellor
- The Executive Council
- The Court

Resources

- Desktop,Laptop, Printer,UPS, Projector, Sound Systems, A/V accessories, Mobiles
- Network Devices wired/ wireless (WI-FI)
- CCTV devices and surveillance system
- Internet and Intranet Access
- Official Websites, web applications
- UMS Portal
- Official Email services
- Mobile Apps
- Data Storage
- Teaching Learning Tools & Resources including Smart Classrooms

IT policies may be classified into the following groups:

- IT Hardware Installation and Maintenance Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Video Surveillance management/ usage Policy (CCTV)
- Digital Display Board (Signage Usage policy)
- Web Site Hosting Policy
- Application Servers management/usge policy
- University Database Use Policy
- End Users Groups (Faculty, students, Senior administrators, Officers, Project Fellows and other staff)
- Network Administrators

1. IT Hardware Installation and Maintenance Policy

1.1 Installation:

- All IT related gadgets and hardware are to be installed and maintained under the control and supervision of University Computer Centre.
- On delivery of any IT products directly purchased by Department/Section, the concerned department will report the same to the Computer Centre with supporting papers like P.O. etc. Computer Centre will engage technical manpower if necessary to supervise the remaining process of installation, site-preparation advisory, certification of specifications, University ID number allocation, Central Stock entry etc.
- All IT gadgets purchased centrally and allotted to various departments will also be supervised and maintained by the University Computer Centre.

Members of University network user community need to know their user status and observe certain precautions while getting their computers or peripherals installed so that they may face minimum inconvenience/ interruption of services due to hardware failures.

[Definition of Users category

Who is Primary User

An individual in whose room the computer or any other IT hardware is installed and is primarily used by him/her, is considered to be ***"primary" user****. If a IT hardware has multiple users, none of whom are considered the "primary" user, the department Head of the concerned department should make an arrangement and make a person in-charge of the common hardware who is to be responsible for compliance with the University IT Policy.*

What are End User Computer/ IT Systems

Apart from the client PCs used by the users, the university will consider Servers, Projectors, Laptops, UPS, not directly administered by Computer Centre, as end-user computers/ IT hardware. If no primary user of such items can be identified, the concerned departments must assume the responsibilities as end-users. The HOD identified persons are accountable for the total stock of the IT hardware in the department, in this category.]

1.2 Warranty & Annual Maintenance Contract

Computers/any other IT hardware purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under Annual Maintenance Contract (AMC) until the product is either declared as obsolete is not repairable/scrap.

The Maintenance of Desktops/Laptops/Server/UPS/Printers etc. should be controlled and managed centrally under the Computer Centre by deploying suitable vendor through tender process as per rule. Such maintenance should include OS re-installation and checking virus- related problems, Internet operation etc. or as per agreement duly agreed upon and signed by the vendor and the University during the contract period.

1.3 Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the ONLINE UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points with Generator Connection that are provided with proper Earthing and have properly laid electrical wiring.

1.4 Operating Environments for Computers:

All servers should be installed strictly in a dust free, moisture free and Proper Air-conditioned environment. However, the Desktop/Laptop should be operated in dust free and moisture-free environment.

1.5 Network Connection --WIRED / Wireless :

While connecting the computer or any other Network devices to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected. For Wire/ Wireless connection, Computer Centre is the regulating authority in allotting/ authenticating various network services, IP addresses, access controls etc. LAN/Internet Services will be authenticated by appropriate authentication server.

1.6 File and Print Sharing Facilities :

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with 'read only' access rule.

1.7 Allotment of Assets ID and Stock Maintenance:

Each and every IT asset installed in the University campus will have an Unique Assets ID clearly written by marker pen/sticker on cover of the main asset so that it is visible and not removable. The Assets ID will be allotted by the Registrar / Finance Department or as may be decided from time to time. Proper stock entry is to be maintained in digital form by the Computer Centre and the concerned user Department or as may be decided by the authority.

1.8 Shifting Computer from One Location to Another :

Computer system may be moved from one location to another with prior written intimation to the Computer Centre, as it maintains a record of computer identification/ names and corresponding IP addresses etc.

Noncompliance

VU faculty, staff, and students and any other stakeholder not complying with this computer hardware installation policy may leave themselves and others at risk of IT operation hazards and network related problems which could result in damage or loss of files, inoperable computer, resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole university. Hence, it is critical to bring all computers into compliance as soon as they are recognized as not to be.

2. Software Installation and Licensing Policy

2.1 General Guidelines:

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) purchased and installed by the supplier.

Any computer purchases made centrally should also have all relevant and necessary licensed software installed.

Use of Open Source software(OSS) is always advisable to those who can use it. The University always encourages the use of Free and Open Source Software (FOSS) wherever possible. University Computer Centre will extend necessary technical support in use of FOSS.

The University as a policy, encourages Bulk Campus Licensing policy in cases where a large number. of licenses of a single software like OSS are used in the campus.

Respecting the anti-piracy laws of the country, the University IT Policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, the university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

2.2. Operating System and its Updating

2.2.1 Individual users should make sure that respective computer systems have their Operating System (OS) updated with respect to their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs 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.

2.2.2 University as a policy encourages user community to go for Open Source Software such as Linux, Open office to be used on their systems wherever possible.

2.3 Antivirus Software and its Updating

2.3.1 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.

2.3.2 Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

2.4 Backups of Data

Individual users will perform regular backups of their vital data. Virus infections/ Power fluctuation/failure often destroy data on an individual's computer. Individual user /System-in-Charge of laboratory/ department should ensure that the regular data backup of vital data is taken.

During Installation of Operating System, the users should ensure that a separate disk volume (secondary) is created in the HDD for data storage. The Primary volume should be used only for the Installation of Software.

Noncompliance

Vidyasagar University faculty, staff, and students not complying with this computer licensing policy and safety and security policy leave themselves and others at risk of violating the anti-piracy law of the country and virus infections which could result in damaged or lost files.

An individual's non-compliant computer can have significant adverse affects on other individuals, groups, departments, or even the whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not doing so.

3. Network (Intranet & Internet) Infrastructure and Usage Policy

The University Campus Network Structure with Internet and connectivity provided to any IP devices like Desktop, Server, Laptop, Smart Phone, Tablet, IP Printer, IP Telephone, IP Camera etc through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The University Computer Centre is responsible for the Expansion, ongoing maintenance and support of the Network. Problems within the University's network should be reported to the Computer Centre. For effective usage and healthy network, the following usage policy and regulations are to be complied with :

3.1 Network installation (New project/ Expansion)

Any new network installation/expansion requirements (departmental or in backbone) will be planned/designed and implemented under the guidance of the Network Control Centre of Computer Centre. All such requirements are to be sent to the appropriate authority through Computer Centre for necessary design and estimate. On approval of the authority it will be purchased and implemented as per existing rules of the University.

3.2 IP Address Allocation

- Any computer (PC/Server) that will be connected to the university network, should have an IP address

assigned by the Computer Centre. The Computer Centre will maintain a Static Private IP Allocation system for smooth running of the System without any conflict.

- IP Allocation in Wireless network/ WI-FI devices to be done through DHCP servers.
- All the Public IP range obtained from the ISPs will be allotted suitably for running all the University Applications smoothly.
- An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual.

3.3 Network Control Centre/ Gateway level access configuration and control

- All the Internet Connections from various ISP's will be terminated at the Network Control Centre/ Gateway Lab under computer centre hereinafter called NCC. Campus-wide Internet Services will be extended from the 'NCC' only through appropriate access control.
- Individual departments/section/centres will not be able to procure independent internet connection for their department.

3.4 Internet Usage Policy

3.4.1 The Internet Connection to University Desktop, Servers, Laptops, Smart Phones and other devices will be enabled through Wired/Wireless connection in the campus.

3.4.2 Internet Services is an essential service now and therefore be made available in the campus without interruption 24×7×365.

3.4.3 The University will have at least two internet bandwidth. One to be used as Primary connection and another as Secondary connection. Necessary load balancing is to be done.

3.4.4 Appropriate service level Internet access Policy will be imposed by the Centre depending upon the user group.

3.4.5 For effective and proper utilization of available internet bandwidth, various levels of access control may be imposed for different types of User groups.

3.5 DHCP/ Proxy / DNS/ ISE Configuration

3.5.1 Use of any computer at end user location as a DHCP /Proxy/DNS/ISE server to connect to more computers through an individual switch/hub and distributing IP addresses should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university.

3.5.2 Gateway level access control may be imposed through ISE, Firewall and Core-Switches.

3.5.3 University Computer Centre will centrally manage these Network services through Central Network Servers.

3.5.4 Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

3.5.5 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.

4. Wireless Local Area Networks policy

4.1 This policy applies, in its entirety, to each academic department, administrative department, Residential Area's Wireless Local Area Network.

4.2 Complete Campus WI-FI is managed and controlled by the Computer Centre. New Installation/ Extension of Wireless LAN, installation of Access point, Controller, creation and management of SSID will be under

the control of the Computer Centre.

4.3 Individual user category-wise SSID may be created like FACULTY, STAFF, STUDENT, SCHOLAR. The Management SSID will be used by Officials. There will be separate SSID for the Hon'ble Vice-Chancellor. Guest SSID will be accessed by Guest with proper authentication.

4.4 The requisition of such extension/new installation is to be brought to the notice of the Computer Centre. After approval from the authority, the execution work will be carried out.

4.5 All the access to wireless network will be user/IP/MAC based authentication in the authentication server.

4.6 All the students, faculty, staff and guests may have WI-FI facility in one mobile, one laptop and one Desktop (Maximum 3 devices).

4.7 All users have to apply for WI-FI access in their devices through proper channel in a prescribed format to be made available in the Computer Centre and website.

4.8 Appropriate access control policy for various WI-FI users group will be imposed by ISE and Firewall for restricted access to unwanted sites.

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

5. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic and other official purposes in the subdomain **mail.vidyasagar.ac.in**

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to **http://mail.vidyasagar.ac.in** with their User **ID** and **password**. For obtaining the university's email account, user may contact Central Library for email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

5.1 the facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

5.2 using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

5.3 All email communication (including any attachment/s) is intended only for the use of the addressee(s) and should contain information that is PRIVILEGED AND CONFIDENTIAL. Unauthorized reading, dissemination, distribution, or copying of the communication is prohibited.

5.4 Any views or opinions or contents presented in email are solely those of the author and do not necessarily represent those the University.

5.5 while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

5.6 User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should

get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.

5.7 User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

5.8 User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

5.9 While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

5.10 Impersonating email account of others will be taken as a serious offence under the university IT security policy.

5.11 Any Spam mail received by the user into INBOX should be forwarded to administrator and then deleted from account

The above laid down policies are broadly applicable even to the email services that are provided by other sources such as hotmail.com, yahoo.com, gmail.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

6. Web Site Hosting Policy

6.1 Official Pages

Sections, Departments, and Associations of Teachers/Employees/Students may have pages on Vidyasagar University official Web page.

Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting. The content must be updated regularly with up to date information. All irrelevant information must be removed from the site to avoid confusion/miscommunication.

As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., http://www.vidyasagar.ac.in only.

For cases in which any department wants to publish notification/any other content, the concerned HOD will send the requisition to the webmaster along with link title, link content and expected location of publication through Email or note-sheet. The responsibility of publishing/updating any content lies on the concerned HOD who has requested the publication/updation.

6.2 Departmental Pages:

Individual departmental web pages may be created and allowed to be published in the website. The content in the departmental page may be added, modified and updated by the concerned department and the responsibility towards that end lies with the concerned department.

6.3 Personal Pages:

The university computer and network infrastructure is a limited resource owned by the university. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal academic pages linked to official web site of the university by sending a written request to the webmaster giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the University. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political

lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups. The hosting of personal web pages along with its initial contents must be duly approved by the authority and it will be maintained by the concerned individuals only.

Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the university.

6.4 Student Web Pages

6.4.1 Though the university does not have this facility as on this date, this policy relates to future requirements for personal student Web pages. Policies for student pages authored as a result of academic assignments are in II above. It is recognized that each individual student will have individual requirements for his/her pages. As the university's computer and network infrastructure is a limited resource owned by the university, only web pages of students related to their assignments will be accepted on the Students web pages. The contents of personal pages hosted by the students even on outside web site must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws.

The following are the storage and content requirements for personal student Web pages:

6.4.2 Servers:

Pages will be placed on the student information server.

6.4.3 Maintenance:

Pages published on the student information server will be maintained under the default rules for personal student pages.

6.4.4 Content Disclaimer:

Every personal page will include the SUK Content Disclaimer (the content disclaimer will be generated automatically).

6.4.5 Responsibilities of Those Maintaining Web Pages:

Sections, departments, units, and individuals are responsible for maintaining their own Web pages.

VU Web pages (including personal pages) must adhere to the VU Web Page Standards and Design Guidelines and should be approved by VU Web Pages Advisory Committee.

6.3 Hosting site/applications under a Sub domain:

6.3.1 Sub-domains under vidyasagar.ac.in may be created to host a specific application with the recommendation of the ICT & MIS Working committee duly approved by the authority. Presently existing sub-domains are dde.vidyasagar.ac.in, eclassroom.vidyasagar.ac.in, ecircular.vidyasagar.ac.in, library.vidyasagar.ac.in.

6.3.2 All in-house application and network servers be preferably hosted centrally at the NCC under Computer Centre for the better security implementation/ management and cost effectiveness.

6.3.3 All applications to be used by stakeholders should preferably be configured for public access from outside the campus with appropriate Public IP address allotment and configuration.

6.3.4 University Portal Application Server will be locally hosted on a subdomain at NCC of the Computer Centre. The Portal will always be integrated with all individual applications running in the campus at any point of time.

7. University Database Use Policy

This Policy relates to the databases maintained by the university administration under the university's e-Governance portal.

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential.

Vidyasagar University has its own policies regarding the creation of database and access to information and these policies outline the university's approach to both the access and use of this university resource.

7.1 Database Ownership: Vidyasagar University is the data owner of all the University's institutional data generated in the university.

7.2 Custodians of Data: Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

7.3 Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

7.4 MIS Components: For the purpose of e-Governance, Management Information System requirements of the university may broadly be divided into seven categories. These are:

- Human Resource Information Management System (HRIMS)
- Students Information Management System. (SIMS)
- Financial Information Management System (FIMS)
- Assets Management System (AMS)
- Project Information Management system (PIMS)
- Library Information Management System ((LIMS)

All these MIS components will come under the UMS Portal in Phases.

7.5 Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.
2. Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only.
3. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the State Public Information Officer of University.
4. Requests for information from any courts, attorneys, etc. are handled by the Registrar's Office of the University and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for response.
5. At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.
6. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar, Director of IQAC, Development Officer, Controller of Examinations and

Finance Officer of the University. The Head of the Department from which the data is sought, will supply it's certified copy.

7. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

8. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but is not limited to :

   - Modifying/deleting the data items or software components by using illegal access methods.
   - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
   - Causing database or hardware or system software to crash, thereby destroying the whole of or part of database, deliberately with ulterior motives by any individual.
   - Trying to break the security of the Database servers.

Such data tampering actions by university member(s) or outside member(s) will result in disciplinary action against the offender by the university authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

8. Video Surveillance management/ usage Policy (CCTV)

8.1 The system

8.1.1 The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public Information Signs.

8.1.2 Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation. The location may be recommended by ICT & MIS Working Committee duly approved by the Hon'ble Vice-Chancellor / Executive Council.

8.1.3 Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

8.1.4 Although every effort may be made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

8.2 Purpose of the system

8.2.1 The system has been installed by the university with the primary purpose of reducing the threat of crime generally, protecting the university premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individual's privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment.

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking.

8.3 The Control Room Operation and Live Viewing

8.3.1 The entire implementation/operation/maintenance of the system will be looked after by the Computer Centre or as may be decided by ICT & MIS working Committee / the Hon'ble Vice-Chancellor.

8.3.2 Images captured/recorded by the system will be monitored and recorded in the Security Control Room which may be located at a location as may be decided by the relevant Committee. Control room may be located at Computer Centre where all recording devices are installed. It may also be located at Security Control Office.

8.3.3 The Surveillance system and control room will run 24 ×7×365

8.3.4 For regular maintenance operation and breakdown of cameras, It cannot be guaranteed that all the cameras will record 24×7. If such situation arises, it is to be reported to Authority on a monthly basis.

8.3.4 No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, and any other person with statutory powers of entry.

8.3.5 The Live Viewing permission to the concerned Head of the department or security may be granted only with the decision of ICT & MIS working committee and permission of the Vice-Chancellor. Backup viewing will not be permitted on live view location.

8.3.6 The CCTV footage may be obtained from the Computer Centre/control room for specific time period only with the permission of the Hon'ble Vice-Chancellor for the purpose of investigation into any incident.

8.3.7 Footage will not be delivered to outsider/media without permission.

8.3.7 All maintenance related issues will be monitored from the Control Room/Computer Centre.

8.4 Recording

8.4.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

8.4.2 Images will normally be retained for thirty (30) days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

8.4.3 All hard drives and recorders shall remain the property of the university until disposal and destruction.

7.0 Access to images

9. Digital Display Board (Signage Usage policy)

9.1 Vidyasagar University Information Transmission system may be done through deployment of Digital Signage TVs at strategic locations across the campus with the recommendation of the ICT & MIS Working Committee, duly approved by the Hon'ble Vice-Chancellor / Executive Council.

9.2 Client server based information modification and uploading in the system may be followed.

9.3 The Computer Centre will implement and maintain the Signage system and server with the final publishing authority.

9.4 Every concerned department will have an in-charge of the display system who will create the content and upload into the server for publishing.

9.4 The Server admin will verify the content and will finally publish in the display panel group.

9.5 The concerned department will be responsible for the actual content and its impact on the public.

10. Responsibilities of the Computer Centre

10.1 Campus Network Backbone Operations

10.1.1 The campus network backbone and its active components are administered, maintained and controlled by THE COMPUTER CENTRE.

10.1.2 THE COMPUTER CENTRE operates the campus network backbone such that service levels are maintained as required by the University Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

10.1.3 The Devices and Services to be maintained at present by The Computer Centre under the Network backbone include, WI-FI Internet service, Wire Internet Services, University e-Governance Portal Management Services, Network and Application Servers, Internet Connectivity, IPCCTV Surveillance System, VOIP and Video Conferencing Services, Virtual Remote Classrooms etc.

10.2 Network Expansion

Major network expansion/upgradation is also the responsibility of the Computer Centre. In Every 3 to 5 years, the Computer Centre reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by the Computer Centre when the university makes the necessary funds available. The expansion/upgradation proposal initiated by the Computer Centre will be duly recommended by the ICT & MIS Working committee and approved by Vice-Chancellor for acceptance.

10.3 Wireless Local Area Networks

10.3.1 Where access through Fiber Optic/UTP cables is not feasible or where the requirement of Wireless network is very vital, in such locations Computer Centre and ICT & MIS Working Committee considers providing network connection through wireless connectivity.

10.3.2 The Computer Centre is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from the Computer Centre prior to implementation of wireless local area networks.

10.3.3 The Computer Centre is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

10.4 Electronic logs

At least one month's Electronics- logs be kept in the Log server in the Computer Centre

10.5 Global Naming and IP Addressing

The Computer Centre is responsible for providing a consistent forum for the allocation of campus network services such as IP addressing and domain name services. It monitors the network to ensure that such services are used properly.

10.6 Providing Net Access IDs and email Accounts

Computer Centre provides Net Access IDs upon receiving the requests from the individuals on prescribed proforma.

10.7 University Data Centre: University Portal Management

University Data Centre is located in the Network Control Centre of the Computer Centre. Its security, configuration, management is the responsibility of the Computer Centre. University Portal MIS system will be under the control and management of the Computer Centre. Necessary Hardware Infrastructure may installed

locally at Data Centre of the Computer Centre. All necessary Security implementation and Data Security is the responsibility of the Computer Centre.

10.8 Centralised Maintenance of University IT Hardware Infrastructure:

The Computer Centre is responsible for the centralised maintenance of all IT infrastructure including Servers, Desktop, Laptop, Printer, Projector, Thin Clients, UPS, Official Mobiles, Tablet, Photocopying Machine, CCTV, LAN & WI-FI infrastructure, Digital Signage System, Smart and Virtual Classroom infrastructure with the deployment of a residential third party vendor to be selected through e-Tender Process at regular intervals.

All related complaints will be sent to the Computer Centre or directly to the residential vendor's office. The vendor will attend the call within 1 hour for addressing the complaint.

All IT related contingency and Upgradation requirements of the various departments may be sent to the Computer Centre for meeting the requirement.

10.9 Authorised Software Installation and Licensing Management.

The Computer Centre maintains the licensing and renewal of various system and Application Softwares. Its service engineers or the external service engineer should not encourage installing any unauthorized software on the computer system(s) of the user(s). They should strictly refrain from obliging such requests.

10.10 Centralised operation and maintenance of IP CCTV Surveillance

10.10.1 The Computer Centre is responsible for operation of the existing setup including live view, maintenance, backup and video data security.

10.10.2 All new installation will be executed by the Computer Centre with the due approval of the University authority.

10.10.3 The Computer Centre will maintain the licensing and renewal of various system and Application Software related to the surveillance.

10.11 Smart and Virtual Classroom allocation, maintenance and management

The Computer Centre is responsible for the overall management, operation and maintenance of all existing Smart and Virtual Classrooms and proposed e-Classrooms.

All these classrooms may be allotted for Regular Classes, Seminar, Workshops, Conferences, Special Lectures, Ph.D. viva-voce etc, Remote and virtual classes, etc.

The interested department must apply online for booking time slots for these rooms. Allotment of time-slots shall be made on the basis of availability and necessity.

10.12 e-Waste Disposal

The Computer Centre, with the assistance of the Garbage disposal authority will ensure that e-wastes are safely disposed off the campus at regular intervals as per e-waste disposal cycle.

11.0 Responsibilities of Department or Sections

A. Accountability of Departmental IT Infrastructure and Stock Register

1. Every Department will assign an in-charge of the IT infrastructure who will be responsible for accountability of the IT components in the Department.
2. Each departmental IT Infrastructure, allotted by the University are to be maintained properly. Each Department/Section will ensure smooth functioning of the Infrastructure.
3. Each Department/Section will maintain the IT Stock Register. Any New Purchase / allotment from the University, is to be properly entered into the Stock Register.
4. Each Department/Section will maintain a Logbook for the Computer Laboratory usage and any

problem (Hardware/software) faced by end user is to be recorded in the logbook.

5. Any major problem/new requisition will be reported by the Head of the Department through the Departmental Committee to Computer Centre for further necessary action.
6. Any IT infrastructure which are not operational/obsolete may be reported to the Computer Centre for necessary inspection and subsequently declaring as Scrap for the next cycle of the e-garbage disposal system.
7. All complain related to WI-FI, CCTV, A-V system, Internet etc. is to brought to the notice of the Computer Centre for addressing the problems.
8. All departments will follow the central e-waste disposal cycle for safe disposal of e-wastes.

B. User Account

Any Centre, Department, or Section or other entity can connect to the University network/ WI-FI using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university or by allocation of statically assigned IP Address. The user account will be provided by the Computer Centre, upon filling up the prescribed application form and submitting it to the Computer Centre.

C. Supply of Information by Section, Department, or Division for Publishing on /updating the VU Web Site

All Schools/Centers, Departments, or Divisions should provide updated information concerning them periodically and upload their documents/resolutions on the University web site.

Hardcopy of such information duly signed by the competent authority at Section, Department, or Division level, along with a softcopy to be sent to the webmaster. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by each Section, Department, or Division.

E. Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the University IT Security Policy. All network security incidents are resolved by coordination with a Point of Contact (POC) in the originating department. If a POC is not available for contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

F. 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 the Computer Centre.

Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but is not limited to,

- Removal of network inlet box.
- Removal of UTP cable from the room.
- Opening the rack and changing the connections of the ports either at jack panel level or switch level.
- Taking away the UPS or batteries from the switch room.
- Disturbing the existing network infrastructure as a part of renovation of the location. The Computer Centre will not take any responsibility for 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 Section, Department or individual user should strictly

adhere to the university network policy and with prior permission and approval from the competent authority and the Computer Centre.

University Network policy requires the following procedures to be followed for any network expansions:

- All the internal network cabling should be as on date of CAT 6 UTP.
- UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.
- UTP cables should be properly terminated at both ends following the structured cabling standards.
- Only managed switches should be used. The Installation and configuration of New network will be governed by the Computer Centre.

12. Responsibilities of the Administrative Units

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

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

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

Hard copy of the information that is supplied by the concerned administrative unit duly signed by the competent authority along with its soft copy (either on mobile storage devices or mobiles or PDA or by email) should be sent to the Computer Centre so as to reach the above designated persons.

13. Regulations on IT Asset ID Allocation and naming:

1. In order to troubleshoot network problems and provide timely service and accountability of the IT assets, it is vital to be able to quickly identify computers and other IT assets that are on the campus network. All computer names on the campus network must use the University standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of the Computer Centre.
2. Finance and audit section will allot Asset ID following the specified naming convention and the Computer Centre will update the same in the Digital Central Stock.

14. Regulations for Desktop Users

These guidelines are meant for all members of the VU Network User Community and users of the University network.

Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security. The following recommendations include:

1. All desktop computers should have the latest version of antivirus such as and should retain the setting that schedules regular updates of virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The

frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine.

Whenever possible, security policies should be set at the server level and applied to the desktop machines.

3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
4. The password should be difficult to break. Password, defined as:
   i. must be minimum of 6-8 characters in length
   ii. must include punctuation such as ! $ % & * , . ? + - =
   iii. must start and end with letters
   iv. must not include the characters # @ ' " `
   v. must be new, not used before
   vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.
   vii. passwords should be changed periodically and also when suspected that it is known to others.
   viii. Never use 'NOPASS' as your password
   ix. Do not leave password blank and
   x. Make it a point to change default passwords given by the software at the time of installation
5. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.
6. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).

When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

7. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
8. All O/S should be licensed. VU has agreement with Microsoft for Campus Licensing. All end user with proper Desktop ID may get the License Key from the Computer Centre.
9. In addition to the above suggestions the Computer Centre recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise.

Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

15. Regulation on Smart Card based access and usage policy

1. All Employee (Permanent/ Temporary/Contractual) and students are eligible to obtain Smart Card for supplying and access to information from/to the University MIS Portal. Smart card may also be used as Unique Identity Card.
2. Smart card issue/re-issue and corresponding information management will be under the control and supervision of Computer Centre.
3. Smart Card holder may use their card for accessing various Access devices for availing Smart card services

as may be implemented from time to time.

4. Smart card validity for permanent employees will be up to the age of superannuation and for the temporary employees it may be as per decision taken by authority from time to time/ case to case.
5. In the event of loss of card, Change of designation due to Fresh appointment to the fresh post/ CAS/PROMOTION, change of validity period, the Smart card may be reissued on receiving with valid reasons. Smart card will be reissued free of cost in case of first loss of card in the complete service period. However, for subsequent losses, the employee have to pay token amount as may be decided by authority.

16. Regulations for use of Smart and Virtual Classrooms

1. All Faculty members will use the Smart and Virtual Classrooms extensively for the teaching- learning process.
2. Faculty members will book the Smart and Virtual Classrooms through Online process for PG Classes at the beginning of a Semester following the guidelines as may be decided from time to time and accordingly, the classes will be reflected in the Semester Class routine.
3. The Smart classes may also be booked for Meeting/Seminar/Workshop and other purposes on payment basis.
4. The smart class with all its component will be handed over to the concerned faculty before the class and taken over after the class by the Technical person engaged for the purpose on behalf of the Computer Centre.
5. All faculty members should be aware of the use of various tools in the smart class. All faculty members may attend awareness programme organised by the Computer Centre from time to time in this regard.
6. Recording of classes may be done with due consent from the concerned faculty member.
7. All Technical support during the class, will be provided by the Computer Centre.

17. Regulations on New Purchase and Central IT Stock

17.1 All Central Purchases will be done upon the Recommendation of the ICT & MIS Working Committee, duly approved by the Hon'ble Vice-Chancellor.

17.2 ICT & MIS Working Committee with due approval from the Hon'ble Vice-Chancellor, will forward the requisition to the Appropriate authority for funds. After the approval of source of fund, the Purchase process may be initiated as per the existing rules.

16.7 All the IT equipment purchased for allotment / installation at various locations will be duly entered into the central Stock Registrar in digital form and allocated Asset ID as per rules of the University.

18. Regulations on e-Garbage Management and Disposal cycle

VIDYASAGAR UNIVERSITY

E-WASTE MANAGEMENT AT VIDYASAGAR UNIVERSITY

18.1 University e-Waste Management and disposal will be done by the above mentioned Management cycle.

18.2 University e-waste management follows responsible re-use and responsible disposal system.

18.3 The e-waste management and control will be done under the supervision of Garbage management Committee of the University through the Computer Centre.

18.4 Each Department will follow the above cycle strictly and generate obsolete/ outdated/out of AMC/non-functioning IT components as e-Waste and report to the Computer Centre and convener of the Garbage Management Committee.

18.5 E-waste will be disposed of from the department every 6 months.

APPENDICES

REGISTRATION FORM

[For Residential Students(Boarders)]

For Network & WI-FI Access for Hostels

1.General Information:

1. Name of the Applicant:	
2. University ID Card No.	
3. Department with semester and roll no.	
4. Contact No.	
5. Email ID	
6. Course Duration	From: To:
7. Residential Address in University (HOSTEL) including room no.	

2. Access Device details:

1. Type of Device (Pl. Tick)	Laptop /Tablet/Mobile /Other
2. Make, Model and Serial No.	
3. MAC / Physical Address	
4. Operating System (Pl. Tick)	Windows / Linux/ Mac/Android/ other
5. Operating System Version:	

3. Declaration:

I hereby declare that the above information is true to the best of my knowledge and belief. I further declare that I accept all the terms and conditions and policies of VU WIFI and I understand that I shall be held responsible for any violation caused by my username. I shall keep my username and password secret and shall not share it with anybody.

Forwarded by HOD Hostel Superintendent Signature of the Applicant
Date:

For Office Use Only

Internet Access Account details	Username:	Password:
IP Address assigned DHCP/Static	DHCP/ Static-	Validity:
Status of Account with Date	Opened on:	Closed on:

APPLICANT'S copy for record [VU- WIFI Internet access]

Name of Account Holder		
Internet Access Account details	Username:	Password:
SSID Allocated		
Account Valid Upto		

Documents to be submitted with this form: University ID card (self attested photocopy)

**Keep this document with you only in safe custody

Verified by the Office of the PG Secretary **Executive Director, Computer Centre**

REGISTRATION FORM

[For Faculty/Officers/Staff/Research Scholar]
For Network & WI-FI Access from Campus

1.General Information:

1. Name of the Applicant:	
2. Department	
3. Designation	
4. Contact No.	Mobile:
5. Email ID	
6. Residential Address in University (IF Staying in University Campus)	

2. Access Device details:

1. Type of Device (Pl. Tick)	Laptop /Tablet/Mobile /Other
2. Make, Model and Serial No.	
3. MAC / Physical Address	
4. Operating System (Pl. Tick)	Windows / Linux/ Mac/Android/ other
5. Operating System Version:	

3. Declaration:

I hereby declare that the above information is true to the best of my knowledge and belief. I accept all the terms and conditions and policies of VU WIFI and I understand that I shall be held responsible for any violation caused by my username/device MAC. I shall keep my username and password secret and shall not share it with anybody.

Forwarded by HOD

Signature of the Applicant
Date:

For Office Use Only

Internet Access Account details	Username:	Password:
IP Address assigned DHCP/Static	DHCP/ Static-	Validity:
Status of Account with Date	Opened on:	Closed on:

APPLICANT'S copy for record [VU- WIFI Internet access]

Name of Account Holder		
Internet Access Account details	Username:	Password:
SSID Allocated		
Account Valid Upto		

Documents to be submitted with this form: University ID card (self attested photocopy)
**Keep this document with you only in safe custody

Verified by the Establishment Section (Emp.ID)

Executive Director,
Computer Centre

Vidyasagar University
Centre for Digital Resource Services
REQUISITION FORM FOR E-MAIL ACCOUNT (Scholars)
(USE BLOCK LETTERS ONLY)

1. Full Name: _____
2. Department: _____
3. Year of Admission : _____
4. Permanent Address : _____
5. Local Address : _____
6. Mobile No. (Mandatory) : _____
7. Existing Email ID (Mandatory) : _____
8. Identity Card No. : _____(Attach Xerox Copy)
9. Please specify the E-mail Account Name you wish to have

   Option one

														@mail.vidyasagar.ac.in

   Option two

														@mail.vidyasagar.ac.in

Declaration

The above information furnished by me is correct, and I undertake to abide by the rules and regulations of the University for proper use of email facility for my research work purpose.

Date : **SIGNATURE OF THE STUDENT/SCHOLAR**

Application for email account recommended by Prof / Dr / Mr / Ms / Mrs.....

Signature & Stamp of

Supervisor/ Head

Office Use Only

The following email ID is created for Dr./Mr./Ms_____

_____on _____

r	s															@mail.vidyasagar.ac.in

Attach photo copy of University Identity Card.

Ph.D. registration certificate also required for research Scholars.

Vidyasagar University
Centre for Digital Resource Services
REQUISITION FORM FOR E-MAIL ACCOUNT (Staff Only)
(USE BLOCK LETTERS ONLY)

1. Full Name: _____
2. Designation: _____
3. Dept./School/Centre: _____
4. Office Telephone Nos. : _____
5. Existing Email ID (if Any) : _____
6. Mobile No. (Mandatory) : _____
7. Employee Code : _____ (Attach Xerox Copy of the University ID card)
8. Please specify the E-mail Account Name you wish to have

   Option one

														@mail.vidyasagar.ac.in

   Option two

														@mail.vidyasagar.ac.in

Date :

Signature

User Counterfoil

The following email ID is created for Prof./Dr./Mr./Ms_____

_____on _____

																@mail.vidyasagar.ac.in

Attach self attested photo copy of University Identity Card and Joining Letter.

Centre for Digital Resource Services

Vidyasagar University, Midnapore - 721102

Registration Form for Remote Access

1. General Information			
Name (IN BLOCK LETTER)			
Library Card No	(At the reverse of the Card , eg. RSANMA120001)		Sex - Male / Female
Faculty / Guide Name			
Type of Appointment	Permanent ☐ Temporary ☐		Valid Up to ___/___/_____
Type of User	Faculty / Staff / Scholar / Student / Other (Specify)		
Course Duration#	From		To
Department			Date of Birth
Contact	Land No.		Mobile No.
2. Technical Information (Must Specify For Remote Access)			
Type of Device	Laptop/Tablet/Mobile/Others(Specify)		
Make & Model			Serial No. -
MAC/ Physical Address			
Operating System (With Version e.g Windows 7)	Windows / Linux / Mac/ Android /etc		
3. Type of E-Resource			
UGC Infonet E-Journal	Please put tick (if you want to avail this facility)	YES ☐	NO ☐
University Subscribed E-Books	Please put tick (if you want to avail this facility)	YES ☐	NO ☐
CD/DVD Mirror Server	Please put tick (if you want to avail this facility)	YES ☐	NO ☐
Intranet Server Access	Please put tick (if you want to avail this facility)	YES ☐	NO ☐
Others			

I hereby declare that the above Information given by me is true. I acknowledge that this account shall be used solely in the performance of my authorized job functions. I also acknowledge that I will take necessary precautions to maintain the confidentiality of my ID & Password; and that I will immediately report its disclosure or use by anyone other than myself, to System Administrator / Deputy Librarian of Central Library, Vidyasagar University. I accept all the terms and conditions and e-resource access policies as declared by CDRS and here by take the responsibility for any violation caused by my username.

Signature of the Faculty /Staff / Scholar

(Please submit Office order / Joining report Along with Form)

Date

For Office Use Only

Account Details	Username:		Password:
IP assigned: DHCP/Specific IP:		Expiry : Never / Specific date 30.06.201	
Status of Account with date	Opened on:		Closed on:

Applicant's copy

Account Details	Username:	Password:
Name of Account Holder		
Account Valid Upto	30.06.201	

Signature of I/C (CDRS)

VIDYASAGAR UNIVERSITY
Midnapore – 721 102
West Bengal

Phone: (03222) 298332/ 298272
Fax No.: (03222) 275329
Website:vidyasagar.ac.in

Application form for University ICT support/service for holding Online seminar, conference, workshop, meeting etc

To
The Executive Director
Computer Centre
Vidyasagar University

Dear Sir,

Kindly provide necessary technical support to the undersigned for organizing/holding a Online Event to be held on.....(date) at.....am/pm.

All details are provided below :

1. Type of the Online Event (Pl. tick) : Seminar /Conference / Worlshop / Meeting / Special Lecture /Other
2. Name / Title of the Event:
3. Name of the organizer (HOST) with Full designation and Department:
4. Start Date and Time of Event:
5. Duration of the programme: …… hrs
6. Type of Support /Platform required: Google Meet / Webex Meet /Youtube Live : (pl. consult ICT section before selecting available platform)
7. Whether necessary expenses to be paid or free service sought :

I do hereby declare that I shall use the above ICT service for the academic purpose only. I also understand that I shall be held fully responsible for any infringement upon cyber security, the university's reputation and violation of the ***"Vidyasagar University IT POLICY, Rules and Regulations 1.0".***
I further declare that the Online event Link shared by the ICT department to the Organiser is confidential in nature and will only be shared to the registered bonafide participant as is approved by the Organiser/ HODs.

Name of Applicant / HOST:

Designation:

Signature:

Date:

Forwarded by
.....

Approved/Not approved
Vice Chancellor

Details of fees, if applicable:

ADDENDUM

- A new item "Virtual Online Teaching and Meeting Applications" has been included under Resources para in Page 3 of "Vidyasagar University IT POLICY, Rules and Regulations 1.0" document

- A new section in Page 7 of "Vidyasagar University IT POLICY, Rules and Regulations 1.0" document has been included as follows:

Section 3.6 : Virtual Online Teaching and Meeting Applications Usage Policy

The University have been using and will continue to use a number of Online teaching tools and Virtual online applications for online classes, Webinar, Workshops, administrative meetings, Viva Voce, examinations etc. The selection of online tools, renewals, usage policy etc. are govern by this policy as follows.

3.6.1 The Purchase/ renew / change of online virtual application tools for the above purpose will be done with the Approval of the Authority as may be required from time to time. The University may adopt google meet, CISCO Webex platform for such application. Other applications may also be permitted in due course of time.

3.6.2 The user/individual hosting the platform officially under University support for the above purposes will apply in prescribed form as in appendices along with the User/participants details. After due approval of the Authority, the events may be hosted officially with complete University ICT Support.

3.6.3 For Online Classes, the classes may be hosted by individual teachers through his own accounts as per the class routine as may be approved by the authority.

3.6.4 University/host will have the authority to record the online virtual event with due consent of majority members prior to the start of the meeting. The recording may be used for future reference only for official purpose.

- "Application form for University ICT support/service for holding online seminar, conference, workshop, meeting etc." has been included in Page 26 of "Vidyasagar University IT POLICY, Rules and Regulations 1.0" document.

- Amended policy of the "Vidyasagar University IT POLICY, Rules and Regulations 1.0" will be read as "**Vidyasagar University IT POLICY, Rules and Regulations 2.0**" henceforth.

This document has been approved by the competent authority and printed by Computer Centre, Vidyasagar University