Sub: Dharmsinh Desai University Information Technology Policy

-:Notification:-

Dharmsinh Desai University (here after referred to as "the University") is involved in multidiscipline teaching learning. Owing to the changing global standards of education & modern practices of online teaching and e-learning, the role of Information and Communications Technology (ICT) in education has become relevant or rather imperative. The IT Infrastructure & ICT Enabling (IIIE) committee of the University is formed to promote the effective use of ICT to support and change the teaching and learning process. The broad objective of the university in forming this committee is to build a strong community of faculty & students which can be largely eased by the use of ICT to attain their goals and reach the next level when it comes to their career. This committee is governed by the information technology policy of the University.

The information Technology (IT) policy document is meant for students, faculty members and all the other employees of the university. This policy document is meant to provide guidance to all stake holder regarding creation, utilization and maintenance of IT infrastructure at DDU. This policy comes into force from the date of this notification.

Date

Dr H M Desai

Vice Chancellor

No: DDU/ITpolicy/

To,

1) Campus director
2) All deans
3) Registrar
4) Coordinator IQAC
5) Administrative officer
6) Accounts officer
7) Coordinator IT infrastructure and ICT enabling committee

Dharmsinh Desai University, Nadiad

IT Infrastructure & ICT Enabling Committee

Preamble

Owing to the changing global standards of education & modern practices of online teaching and e-learning, the role of Information and Communications Technology (ICT) in education has become relevant or rather imperative. The IT Infrastructure & ICT Enabling (IIIE) committee of the University is formed to promote the effective use of ICT to support and change the teaching and learning process. The broad objective here is to build a strong community of faculty & students which can be largely eased by the use of ICT to attain their goals & reach the next level when it comes to their career.

Scope of Work

1) Facilitate paperless information exchange across departments by provisioning of fast and secured Internet access within the campus. This includes requirement gathering, budgeting, procurement, and deployment of adequate and efficient IT infrastructure like Network Servers, Routers, Switching, Cabling, etc.
2) Facilitate electronic storage of data centrally by means of NAS or other web storage facilities. Also to restrict data access only by authorized users by means of Data security tools and enforcement of IT usage policy.
3) Ensure preventive maintenance of ICT infrastructure & Facilitate in-time repair of the IT resources.
4) Create a facility for Employees' Biometric Attendance from the HR perspective.
5) Facilitate implementation of ERP technology for promoting innovative teaching & learning & administration processes.
6) Facilitate implementation of campus wide Internet access & emailing for current students, employees & visitors.
7) Create a facility for integrating e-resources with conventional classroom teaching by means of smart classrooms or say ICT enabled classroom. It includes the facility for streaming & recording lectures, making interactive and multimedia-enriched teaching material, etc.
8) Create a facility for Securing Access to the server room and other key locations.
9) Create a facility of Mobile charging Station.

DDU Information Technology (IT) Policy

Undoubtedly, Intranet & Internet services have become the most important resources in educational institutions & research organizations. Realizing the importance of these services, DDU took the initiative way back in 2000 and established basic network infrastructure in the academic complex of the university. Over the last two decades, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the university's academic environment. Now, the university has 750+ network connections covering more than Eight buildings across the campus and is expected to reach 1000 connections very soon.

University Computer Centre (UCC) is the department that has been given the responsibility of running the university's Intranet & Internet services. UCC is running the Firewall security, DHCP, email, DNS, and web servers and manages the network of the university. DDU is getting its Internet bandwidth from the Internet Service Provider. Total bandwidth availability from the ISP source is 500 Mbps over Fibre (leased line). DDU has also provisioned 250 Mbps wireless connectivity in case of fiber failure. While educational institutions are providing access to the 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 users:

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

Intent

Since a limited amount of personal use of these facilities is permitted by DDU to users, including computers, printers, e-mail, and Internet access, therefore, it is essential that these facilities are used responsibly by users, as any abuse has the potential to disrupt DDU image and interfere with the work and/or rights of other users. It is therefore expected of all users to exercise responsible and ethical behavior while using DDU's IT facilities. DDU recognizes the vital role information technology plays in education as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by DDU's IT resources authorized users, the need for an increased effort to protect the information and to provide adequate technology resources that support it, is felt by DDU.

The use of the DDU's IT resources for limited personal use is a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the DDU's

IT resources efficiently and responsibly. In the absence of clearly defined IT policies, 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 their freedom of users. As IT users are aware, all 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, DDU 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.

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 Information Technology, Information security in general and therefore policies that govern the information security processes 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

The purpose of DDU 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 the University as a whole, departments, and individuals who are part of the 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 the following groups:

- IT Procurement Policy
- IT Usage Policy
- IT Security Policy
- Web Site Policy
- Emergency Management of IT
- Breach of DDU Information Technology (IT) Policy

Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject DDU to any liability.

Scope

It may be noted that DDU IT Policy applies to technology administered by the DDU centrally or by the individual departments, to information services provided by the DDU administration, or by the individual departments, or by individuals of the DDU community, or by authorized visitors including vendors/suppliers providing services to DDU on their own hardware connected to the DDU network. This IT policy also applies to the resources administered by

the central administrative departments such as the Library, Computer Centres, Laboratories, and Offices of the recognized Associations or wherever the network facility was provided by the DDU.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to the campus network are subjected to the Do's and Don'ts detailed in the DDU IT policy. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty, and others who may be granted permission to use the DDU's IT infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by the DDU 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.

It shall be the responsibility of all Faculty Deans and the Head of the Department to ensure that this policy is clearly communicated, understood, and followed by all users. The HR/Admin department and the respective activity in-charges who contract for these services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy & brief them before any access is given to them.

General

Standards for acceptable use of DDU IT resources require

- Responsible behavior with respect to the IT environment at all times.
- Compliance with all applicable laws, regulations, and DDU's policies
- Respect for the rights and property of others including Intellectual Property Rights.

1.1 IT Procurement Policy

The IT resource requirements from each faculty/department should be gathered and the budgetary approval for the same must be obtained annually. All purchases within the allotted budget must be done centrally and should be in line with the purchasing policy of DDU. The technical specifications of major resources shall be concluded in consultation with the IIIE committee of the University.

1.1.1 Hardware Resources

The desktop computer systems must be purchased as a standard desktop system bundle and must be branded systems from an internationally recognized manufacturer. They should be preferably loaded with a free operating system like Linux and integrate with existing hardware deployed at the majority of institutional locations.

The high-end server systems must be branded system from an internationally recognized manufacturer and must be purchased along with requisite software modules. Server systems purchased must be compatible with the institution's other server systems and all other computer hardware in the institution.

Requirements and Specifications for the Networking Hardware (such as firewall, routers, switches, Fiber cables and modules with required accessories, mounting racks, Online UPS, Network Access Storage devices, etc.) must be decided by the DDU Network Administrator in consultation with the IIIE committee of University.

Computer peripherals (such as printers, scanners, external hard drives, Webcam, Head Phones, Speakers, CCTV, and Projectors, etc.) can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals. Computer peripherals purchased must be compatible with all other computer hardware and software in the institution.

1.1.2 Software Resources

DDU encourages and promotes the use of open-source or freeware for academic activities. Open source or freeware software can be obtained without payment and is usually downloaded directly from the internet.

All software including open source or freeware that requires licensing or involves legal implications must be approved by the Head of the respective Department, prior to the use or download of such software.

All licensed software requirements should be reviewed by the central committee and appropriately purchased depending upon the need and budget allocation. All licensed and/or proprietary software must be purchased centrally from authorized partners and distributed to the concerned department or end user.

All software must be appropriately registered with the supplier where this is a requirement. DDU is to be the registered owner of all software. All software must be compatible with the institution's server and/or hardware system.

1.2 IT Usage Policy

It is necessary to ensure that the use of IT resources (Hardware/Software) for all employees within the institution is appropriate. All employees of DDU and the other users must adhere to the IT usage policy before utilizing IT resources within DDU or IT resources owned by DDU at other locations.

1.2.1 Software Usage

Only software obtained in accordance with the DDU's IT procurement policy is to be installed on the institution's computers. Prior to the use of any software, the employee must go through the instructions on any licensing agreements relating to the software, including any restrictions on the use of the software.

All computer software copyrights and terms of all software licenses must be followed by all employees of the institution. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of the Head of Departments to ensure these terms are followed.

Unauthorized software is prohibited from being used in the institution. It includes the use of software owned by an Employee and loading it onto the institution's computer. Software audit of all hardware once a year should be completed to ensure that software copyrights and license agreements are adhered to.

Without approval, software owned by DDU cannot be loaded on an employee's personnel computer that is not owned by the institute. Where an employee is required to use the software

at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, it may be permitted provided there is no restriction of licensing or copyright. In extreme conditions, separate software may be procured for usage at home. Where software is purchased in this circumstance, it remains the property of the institution and must be recorded on the software register.

The unauthorized duplicating, acquiring, or use of software copies is prohibited. Any employee who makes acquires, or uses unauthorized copies of the software will be referred to the IIIE committee of the University for Further Consultation. The illegal duplication of software or other copyrighted works is not condoned within this institution and University is authorized to take disciplinary action where such an event occurs.

For all software including purchased or licensed software applications, and any other software residing on DDU-owned equipment, all users must comply with the software licensing policy and must not use/install/download any software for their individual use without prior approval.

UCC takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property. In case any such software is found on any DDU system which is not allocated to the individual user, it shall be the responsibility of the user to inform the same to department head or higher officials.

1.2.2 Hardware Usage

All the computers and peripherals should be connected to the electrical points that are provided with the proper earthling and have properly laid electrical wiring. While connecting the computer 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 immediate power supply location from where the computer and its peripherals are connected.

An employee is held responsible for the content (in the file storage area, web pages, stored/archived emails, etc.) stored in the allotted IT resource.

Conduct that interferes with the normal and proper operation of DDU information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

1.2.3 Access Control

Users must physically connect or disconnect any equipment, including DDU-owned computers and printers, to or from any DDU network only after permission.

All DDU computers that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.

Only persons who have been authorized can access and/or make emergency changes to any DDU computer system or centralized network devices.

Unless prior approval has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to DDU systems and information. All in-bound connections to DDU computers from external networks must be protected with an approved password or ID access control system.

Modems may only be used at DDU after receiving the written approval of the Vice Chancellor and must be turned off when not in use.

All access control systems must utilize user IDs, passwords, and privilege restrictions unique to each user. Users are prohibited from logging into any DDU system anonymously. To prevent unauthorized access all vendor-supplied default passwords must be changed before DDU's use.

Access to the server room is restricted and only recognized IT staff or someone with due authorization is permitted to enter the room. The server room location is independent and not shared either with UCC or laboratory or classroom.

Users shall not make copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

Users are forbidden from circumventing security measures. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of DDU policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing.

1.2.4 Passwords

Individual password security is the responsibility of each user. The users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.

To ensure that a password is not misused, passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them.

Under no circumstances, users shall use another user's account or password without proper authorization.

Under no circumstances, the user must share his/her password(s) with other users, unless the said user has obtained from the concerned authority the necessary approval in this regard. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.

In cases where no prior approval had been obtained for sharing of password(s) with other users, such user shall be completely responsible for all consequences that shall follow in respect of

breach of this Policy and DDU shall initiate appropriate disciplinary proceedings against the said user.

1.2.5 Internet and Intranet Usage

The campus network backbone and its active components are administered, maintained, and controlled by UCC.

Major network expansion is also the responsibility of UCC. Every 3 to 5 years, UCC reviews the existing networking facilities and the need for possible expansion. Network expansion will be carried out by UCC when the university makes the necessary funds available.

Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of UCC. It essentially means that exactly at which location the fiber optic-based backbone terminates in the buildings will be decided by the UCC. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be fiber optic, wireless, or any other media) is also the responsibility of UCC.

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the UCC. Following a systematic approach, the range of IP addresses that will be allocated to each building block is decided. So, any computer connected to the network from that block will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected may be binded internally with that IP address, with a request to the Network Administrator, so that no other person uses that IP address unauthorisely from any other location.

Use of any computer at the 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 an 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 UCC. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the UCC and after meeting the requirements of the university IT policy for running such services.

Individual connecting to the university network over the WLAN must register for the same with UCC. Network access must be restricted either via authentication or MAC/IP address restrictions or both. If individual department/units wants to have wireless extension over the wired network, prior to installation of such network, it should obtain permission from the university authorities whose application must be routed through the In-charge, UCC.

UCC provides Network Access IDs and email accounts to the individual users to enable them to use the Internet services through campus-wide network and email facilities provided by the university upon receiving the requests from the individuals on prescribed proforma. The credentials provided are not to be shared with any employee within the institution.

Access to the internet and its resources is provided for the academic activities on behalf of DDU. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out into the Network Firewall by the UCC.

Requests for new user-IDs and changes in privileges must be made to the UCC in email (itsupport@ddu.ac.in) with a copy to the respective Head of the Department/Activity In charge. Requesting users must clearly state why the changes in privileges are necessary.

Where an employee forgets the password or is 'locked out', then the DDU Network Administrator is authorized to reissue a new password upon receiving an official email request on itsupport@ddu.ac.in, from the user or an authorized person on behalf.

In response to feedback from the HR/Admin Department, UCC will revoke any privileges no longer needed by users. After receiving information from HR/Admin department all system access privileges will be terminated within 24 hours when a user leaves DDU. DDU management reserves the right to revoke the system privileges of any user at any time.

The DDU IT Support team reserves the right to block access to any Internet resource without any prior notice, in case anyone required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for academic purpose and conducting technical activities. The approval for the same needs to be obtained and intimated through email on itsupport@ddu.ac.in.

To protect DDU's IT systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted.

Institute has procured sufficient bandwidth plan. In order to ensure its maximum utilization for academic activities, software patches or updates may be downloaded with prior intimation to the DDU Network Administrator. While doing so, strict adherence to the vendor's security and usage guidelines must be ensured.

Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the DDU network or the internet or bypass security features.

Use of DDU network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

1.2.6 Email Usage

All authorized users are provided with an e-mail account on ddu.ac.in domain, which is either individual to the specific user or generic email ID and the same is protected with a password which is provided to the individual user. DDU Network Administrator is responsible for the issuing an initial password (that will be required to be changed when the employee logs in for the first time.)

DDU email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. DDU provides the email system for the purposes of conducting

academic & technical activities and it may not be used for personal gain or other activities unrelated to DDU's operations. Users must not use the system to promote an external cause without prior permission from the competent authorities. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by IT department without any prior information, however the same may be re-instated with the approval.

Email users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence exchange of information should be limited to reliable sites. DDU system automatically checks downloaded material for viruses, however, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the IT Support team immediately for inspection and action.

Reasonable personal use of the email system is permitted. Personal use of the e-mail service must not interfere with DDU's operations, involve cost implications for DDU or take precedence over the user's job accountability.

Users are prohibited to use their DDU affiliations and/or DDU email ids in public domain (for personnel & non-academic activities) and/or social forums without prior authorization. Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation of the country or which brings the organization into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via email.

All material contained on the email system belongs to the DDU and users should consider messages produced/received by them on DDU account to be secure. The confidentiality of email data should be maintained by the individual user.

Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties, especially mailing lists.

The above policies particularly are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.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.

1.2.7 Helpdesk Process

All help and support pertaining to the user/network/back-end shall be provided by the IT support staff of the department in consultation with the DDU Network Administrator (applicable only for the department having such staff) or where the local IT support staff are not available, by the DDU IT Support staff. In case any user finds any problem with the IT systems or need any help, they can send in their request to DDU IT Support team via e-mail to itsupport@ddu.ac.in. In the event of emergencies, DDU Network Administrator can be contacted via telephone, however all phone calls must be followed by an e-mail later.

1.2.8 Data Backup

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility for backing up the information located in shared access servers is the administrators.

However, Data Backup in Desktop PC and Notebook is the responsibility of the user to whom the computer has been assigned. It must be borne in mind that not only are hard disks inclined to fail, but also removable storage are quite prone to errors that destroy their contents and/or access, so one need to do the restoration testing time to time basis.

1.2.9 Bring Your Own Device

At DDU, we acknowledge the importance of mobile technologies in improving institution communication and productivity. In addition to the efforts put up for increased use of portable devices, staff members have the option of connecting their own devices to DDU's network and premises. Employees when using personal devices within institution should take prior approval from the Department/IIIE Committee. If required, the DDU Network Administrator may record the device and all applications used by the device.

Personal devices can only be used for the following institution purposes:

- email access,
- Institution internet/intranet access
- Institution ERP system access
- Preparation of various documents & its printing
- Preparation & Submission of information using Institutional network.

All staff who use personally owned notebooks, tablets and other kind of portable devices for institution purposes or access DDU's technology equipment and/or services are responsible for all the content on the personnel devices and especially that which they make available to other users. Each employee who utilizes personal devices within institute must

- Not download or transfer institution or personal sensitive information to the device. Sensitive information includes intellectual property, other employee details etc.
- Not use the registered device as the sole repository for DDU's information. All institution information stored on personnel devices should be backed up.
- Make every reasonable effort to ensure that DDU's information is not compromised through the use of personnel equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected.
- Maintain the device with all legal software and content.
- Abide by DDU's internet policy for appropriate use and access of internet/intranet.
- Notify DDU immediately in the event of loss or theft of the registered device.
- Not connect USB memory sticks from an untrusted or unknown source to DDU's equipment.

All employees who have a registered personal device for institution use acknowledge that the institution

- Owns all intellectual property created on the device

- Can access all data held on the device, including personal data
- Will delete all data held on the device in the event of loss or theft of the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for institution use at any time.

1.3 Information Technology Security Policy

It is very much essential to protect IT assets and resources within the institution to ensure integrity, confidentiality and availability of data and assets.

1.3.1 Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through keypad, smart lock etc. IIIE Committee of University should ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify DDU Network Administrator immediately.

All security and safety of all portable technology, such as laptop, printers, scanners, webcam, speakers, headphones, presenters, iPad etc. will be the responsibility of the employee who has been issued with the laptop, notepads, iPads etc. Each employee is required to use locks, passwords, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, UCC will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage.

All devices, must never be left unattended in a public place, or on a desk in an unlocked office. The shared resources must not be left unattended even if not in a use.

All major IT resources, procured both centrally or by respective department/unit must be recorded in Fixed Asset Register and labeled properly. It is recommended to carry out physical verification of the same on regular basis.

1.3.2 Information Security

It is not the policy of the University to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the University's Internet links.

All sensitive, valuable, or critical institution data is to be backed-up.

It is the responsibility of individual Activity in charges to ensure that data back-ups are conducted on monthly basis in general and on regular interval for examination related information.

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.

All data/application servers that has internet access must have anti-virus software installed. It is the responsibility of the server administrators to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution.

All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. This includes the databases maintained by the university administration under the university's e-Governance.

Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only. 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. However, the personal information of stack-holder may be kept on the website, if approved by the authorities.

Requests for information from any courts, attorneys, etc. are handled by the Registrar 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.

All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Vice Chancellor, Registrar, Director, Controller of Examinations and Finance officer of the University.

Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments, or Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual, or Trying to break security of the Database servers will result in disciplinary action against the offender by the university authorities.

1.4 Website Policy

Website play an important role in showcasing institute in the public domain. It is desire to have functional and well organized website along with all correct and updated information.

1.4.1 Website Register

The website register must record the following details:

- List of domain names registered to the institution
- Dates of renewal for domain names
- List of hosting service providers & hosting capacity.
- Expiry dates of hosting

DDU Network Administrator is responsible for any renewal of items listed in the register.

1.4.2 Website Content

All content on the institution website is to be accurate, appropriate and current. This will be the responsibility of the various activity in charges, Deans and department Heads.

As the university does not have the facility for Web Pages for eLearning as on this date, it is recommended that such information pages should be placed on the student information server. Departments are encouraged to set up departmental servers in the campus itself for eLearning purpose, in consultation with the IT Support Team. However, faculty must be careful that the published material is not misrepresentative in any way by conflicting with official DDU or other Web sites.

All content on the website must follow the uniformity as per the existing content design. Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institution. The content of the website is to be reviewed monthly. The following persons are authorized to direct website administrator for changes to the institution website.

- Registrar
- Controller of Exam
- Faculty Deans
- IIIE Committee of University
- IQAC Coordinator

1.5 Emergency Management of Information Technology

Preventive maintenance and disciplined usage of IT resources is primary key to keep all of them in a usable conditions. However, many times the situation and circumstances are beyond control and demand for Emergency management of all information technology within the institution.

1.5.1 IT Hardware Failure

Where there is failure of any of the institution's hardware, this must be immediately referred to the person in charge for that resource.

Each in charge should undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to institution operations.

1.5.2 Virus or other security breach

Sufficient training should be provided to the local administrator for ensuring that any security breach is dealt with within 1 day to minimise disruption to institution operations.

In the event that the institution's information technology is compromised by software virus or any other malwares, such breaches are to be reported to the local administrator immediately.

1.5.3 Website Disruption

In the event that institution website is disrupted, the following actions (priority in order) must be immediately undertaken:

- Notify the Head of the Department
- Notify the Administrator about the issue.
- Notify the DDU IT Support Team

- Notify the IIIE Committee of University
- Notify the faculty Dean/Registrar/Director
- Notify the Website host

1.6 Breach of DDU Information Technology (IT) Policy

DDU recognize that people make mistakes and employees may not always follow DDU IT policies closely. Any action that may expose DDU to risks of unauthorized access to data, disclosure of information, legal liability, or other potential system failure is prohibited and may result in disciplinary action.

DDU want to give employees a chance to correct their behaviour when possible and assist them in the process. At the same time, it is also needed to ensure that serious offenses are thoroughly investigated and dealt with. Where an employee is aware of a breach of this policy, they are obliged to notify the immediate supervisor. Where there is a breach of policy by an employee, that employee will be referred to the authorities for further consultation.

For that, disciplinary process has six steps of increasing strictness - Progressive Discipline procedure, to address an employee's misconduct particularly in view of the IT Policy. These steps are:

- Verbal warning
- Informal meeting with supervisor
- Formal reprimand
- Formal disciplinary meeting
- Penalties
- Termination

1.6.1 Explaining the Steps

Step 1: When a IT Administrator/Supervisor issues a verbal warning to an employee, they should do so privately. When appropriate, they should provide that employee with a evidence of the policy they violated, and explain progressive discipline steps. Supervisors should provide employees with any coaching or advice they need.
Employees have *two days* to correct their behaviour before step 2 takes effect.

Step 2: A supervisor discusses corrective actions with an employee. Employees should receive actionable feedback on how to deal with an unintentional violation. They can review coaching or mentoring methods.
Employees have *a week* to correct their behaviour before step 3 takes effect.

Step 3: Employees receive a formal written reprimand. Administrative Office should inform them that if they do not correct their behaviour within *one week*, along with justification in writing, step 4 will take effect.

Step 4: Employees will be called in for a formal disciplinary meeting with Registrar, and their immediate supervisor. They will have the chance to explain their side and Registrar is obliged to investigate. Registrar must clarify that this is the final step before an employee is penalized. Employees must correct their behaviour immediately, or step 5 takes effect.

Step 5: This step encompasses any penalties that employees will receive. This usually includes detraction of certain perks and benefits (as long as they are not mandatory by law or funding agencies.) It may also include suspension without pay or demotion for serious offenses. DDU will still provide counselling in this stage if appropriate. DDU will apply this step uniformly and fairly. It will not result in adverse impact for protected groups.

Employees must correct their behaviour within *one month* before step 6 takes effect.

Step 6: Employees who continue to violate our policies, either voluntarily or involuntarily, by this stage will be terminated. This step will follow an official investigation by the Registrar (or legal authorities when appropriate) to ensure that terminating an employee is fair.

All of the above steps are official and the concern officials should document them. HR/Admin office must also keep records of the process from step 3 onwards.

1.6.2 Procedure

DDU Network Administrator, or immediate supervisor should let employees know when they launch a progressive discipline procedure. For example, pointing out a issue is not necessarily a verbal warning. If IT Administrator/Immediate supervisor judge that a progressive disciplinary process is appropriate, they must clarify this to their team member and document the step. The progressive discipline process may begin from a different step, according to the severity of an employee's misconduct.

Each step may be repeated instead of moving forward to the next step at administrative Office or a DDU IT Cell's discretion. For example, a supervisor may choose to have more than one verbal warning (step 1), informal meeting with their employees (step 2) before issue a formal reprimand (step 3.). The supervisors can make the decision to repeat a step if they:

- Feel that the step was not properly executed the first time.
- See signs of improvement in their employee and want to help them further.
- Believe conditions or parameters change enough to make repeating the step necessary.

The disciplinary procedure starts from the step depending on the violation as per the scenario mentioned below.

Violation	Starting Step
Prolonged or intermittent surfing, affecting the quality of work	1
Sharing of harmful and embarrassing content.	2
Confidential information is being made public and/or personal information of stack-holder (other than the personal information, kept on the website) is distributed in any form to outside persons or agencies particularly not authorized for.	3
Disrupt DDU image and interfere with the work and/or rights of other users.	3
Illegal use of software on DDU's IT resources including licensed, open source or freeware that requires licensing or involves legal implications.	2
Use of DDU network resources to illegally use, acquire, distribute or duplicate unauthorized copyrighted or licensed material, except as permitted by law or by the owner of the copyright.	3
Using DDU owned software for individual use without prior approval.	2

Interfering the normal and proper operation of DDU information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others.	2
Physically connect or disconnect any equipment, including DDU-owned computers and printers, to or from any DDU network without approval.	1
Establish Internet or other external network connections that could allow non-authorized users to gain access to DDU systems and information.	3
Access to the server room without due authorization.	3
Make copies of system configuration files (e.g. Passwords, etc) for own, unauthorized personal use or to provide to other users for unauthorized uses.	3
System cracking (hacking), password cracking (guessing), file decryption, computer configuration changing or similar unauthorized attempts to compromise security measures & network performance.	3
Test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing.	2
Share password(s) with other users, unless the said user has obtained from the concerned authority the necessary approval.	1
Violating IP address allocation policy of the university	1
Using DDU affiliations and/or DDU email ids in public domain and/or social forums (without prior authorization.) for personal gain or other activities unrelated to DDU's operations	4
Modifying/deleting the data items or software components deliberately, or Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately, or Trying to break security of the Database servers.	4

This policy is meant to provide general guidelines. DDU reserves the right to treat circumstances in a different way from that described in this policy. It means HR/Registrar can skip any of the steps if they believe they are obsolete. For example, if an employee has received several formal reprimands for the same offense, HR may choose to terminate them directly. Or an employee may be directly suspended for a short period as a punishment. However, DDU is always obliged to act fairly and lawfully and document every stage of the progressive discipline process.

Indemnity

DDU bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify DDU against any and all damages, costs and expenses suffered by DDU arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by DDU.

Exemptions

DDU reserves the right to amend these policies and practices at any time without prior notice. This policy is mandatory unless the Vice Chancellor grants an exemption based on the request.

Dr. H. M. Desai
Vice Chancellor