MAHARSHI DAYANAND UNIVERSITY, ROHTAK

IT Policy

Maharshi Dayanand University's IT Policy

The University, over the last few years, has taken several initiatives to use information and communication technologies for performing administrative functions, financial management, online admissions, examination-related operations, stores management, library operations and services, teaching and research, hostel administration and host of other activities. The implementation of e-governance system is in the final stages. The campus wide network, using state-of-the-art technologies, was established in 2007. Ever since, the use of ICT and network-based services has witnessed phenomenal growth. In view of this, the university administration felt the necessity to formulate its IT policy for ensuring: proper use of IT resources and bandwidth; effective control on the activities taking place on the university's network, whether related to university or not; and security of university's IT-based resources.

A. Objectives of IT Policy:

The University will use IT as a strategic tool to accomplish the following objectives:

1. IT for Teaching-Learning Process and research & Development Activities

The University will develop infrastructure and resources in phased manner as under:

a. Infrastructure

i. ICT will be used in the teaching departments for conducting research and making classroom pedagogy and delivery system more effective and efficient.

ii. ICT will be used in offices for effective and efficient functioning and transparency.

iii. The University will provide a PC/Laptop/Tablet to all teachers for discharging their teaching, research and other official responsibilities.

iv. The University should ensure sufficient number of PCs in computer/ Internet labs of the teaching departments/library for use of students/ research scholars/ teachers/ other university employees.

v. The University would ensure sufficient bandwidth in teaching departments, administrative offices, hostels and residential area for efficient & effective network surfing and other related activities.

vi. The University will acquire high-end systems for advance experiments whenever and wherever required.

b. Resources

i. The existing tools and resources will be upgraded from time to time, and new ones will be identified and procured.

ii. Centralized e-learning resources will be developed and deployed.

iii. Web Portal for accessing internal and external e-learning resources will be developed.

iv. As far as possible, open source software/portals will used. A repository of the same also be created.

v. The university-generated/created resources will be placed in public domain for public welfare, subject to the laws and bye-laws of the University/state/country.

2. IT for Governance Process

a. The entire governance process will be computerized.

b. Help centres/desks will be established for the university stakeholders.

c. The processes for enhanced security, efficacy, efficiency and transparency will be optimized/re-engineered.

d. IT will be used for monitoring & management of university resources.

e. IT will be used for grievance logging & redressal monitoring.

f. Human resource development programmes will be offered from time-to-time to upgrade the skills of the university staff to use ICT.

3. IT for Resource Sharing, Collaboration & Communication

a. Use of Wiki tools for idea/information sharing will be promoted and exploited.

b. Centralized resources will be developed

c. Resource portal will be developed.

d. Collaboration tools & platforms will be developed.

e. Email, Unified Communication Infrastructure will be developed.

B. Scope of the IT Policy

Computers owned by University, whether purchased out of University’s own resources or out of research projects’ funds and their users will be covered by the IT Policy and consequent Do’s and Don’ts. Even the systems owned by individuals, when connected to university network will be subjected to the Do’s and Don’ts detailed in the university IT policy.

Further, the faculty, the students, the staff, the authorised visitors/visiting faculty and others who may be granted permission to use the University’s IT infrastructure, shall comply with the guidelines enshrined in the University’ IT Policy. Offenders of University’ IT policy/Laws and bye-laws enacted by State Government and Central Government shall invite action against them as per laws and byelaws of the University/State/Country.

C. Standard policies and procedures

To achieve the above objectives, the following standard policies/procedures will be followed:

1. Procurement Policy:

a. Purchase procedure prescribed in the University Calendar Vol IV- University Accounts Code will be followed.

b. Hardware & software with standardized specification will be procured for ease of support and resource/knowledge sharing.

c. Attempt will be made to have as long warranty period as possible. After the expiry of warranty period, all the IT equipments should be brought under AMC cover. AMC terms and conditions should be as comprehensive as necessary for maintenance of hardware and software.

d. User requirements for computational power will be determined and met from the existing resources. Procurement will be made for power users and systems with lower computational power will be moved down the requirement chain.

e. For the purpose of asset management, inventory of all IT products will be made in the University's computerized Store Management System in consultation with the University Computer Centre.

f. Green computing will be kept in mind while purchasing IT products.

2. Installation Policy:

a. For every system of the university, some staff will be designated as person responsible for IT policy compliance and proper handling.

b. Only licenced software will be used. Use of pirated software is prohibited.

c. Computer purchases made by the individual departments/PIs, if any, will ensure that such computer systems are pre-loaded with all licensed software - operating system, antivirus software and necessary application software.

d. Respecting the anti-piracy laws of the country, University IT policy does not permit any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any violation, the department/individual shall be held personally responsible.

e. Individual users will be responsible for updation of OS in respect of their service packs/patches through Internet. This is particularly important for all MS Windows-based computers (both PCs and Servers). Updation of 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.

f. 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.

g. Individual users should have regular backups of their vital data, as virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one should have the computer's hard disk partitioned into 2 volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive.

h. University, as a policy, encourages user community to go for open source software to be used on their systems wherever possible.

i. Site licences of the software, being cheaper option, should be purchased wherever possible.

3. System & Network Use Policy

a. 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. As far as possible, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

b. Client machines, where potentially damaging software is found to exist, will be liable to be disconnected from the university campus network.

c. If the client's activity adversely affects the network's performance, such a machine is liable to be disconnected from the university campus network.

d. Access to remote networks using the university network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the university network connects.

e. Use of university network and computer resources for personal commercial purposes is strictly prohibited.

f. Network traffic will be monitored for security and performance reasons.

g. Impersonation of an authorized user while connecting to the university network will amount to violation of the University IT policy. It will lead to termination of the connection and will invite disciplinary/legal action.

h. Computer system should be moved from one location to another with prior written intimation to the UCC, as UCC maintains a record of computer identification names and corresponding IP address. Such computer identification names follow a specific convention. As and when any deviation (from the list maintained by UCC) is found for any computer system, network connection will be disabled. However, connection will be restored on written request of the user by e-mail.

4. E-mail Account Use Policy

a. Communication by e-mail facilitates almost instant delivery of messages and documents to the campus and extended communities or to distinct user groups and individuals. Use of e-mail also results in lot of saving and environmental protection.

b. The university staff will, therefore, use University’s official e-mail services for all official communication by logging on to university website (**http://www.mdurohtak.ac.in) – ‘New mail corner’** with their User **ID** allotted by UCC and **password**.

c. For obtaining the university’s email account, the staff/other users may contact UCC for e-mail account and default password by submitting an application in a prescribed proforma.

d. The staff will keep their e-mail account active by using it regularly.

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

(1) The facility should be used primarily for academic and official purposes, and to a limited extent, for personal purposes.

(2) Using the facility for illegal/commercial purposes is a violation of the university's IT policy. It will entail withdrawal of the facility, besides other disciplinary action(s). The illegal use includes the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages, generation of threatening, harassing, abusive, obscene or fraudulent messages/images, and other acts of similar nature.

(3) While sending large attachments to others, the user will ensure that the recipient has e-mail facility that allows him to receive such large attachments.

(4) User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

(5) 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 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.

(6) User should configure messaging software (Outlook Express/Netscape messaging client, etc.) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer, thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

(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.

(8) User should refrain from intercepting, or trying to break into others email accounts, as it amounts to infringing the privacy of other users and violation of university policy.

(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.

(10) Impersonating email account of others will be taken as a serious offence under the university IT security policy. It will invite legal action against the offender.

(11) It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

f. The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Gmail.com, 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.

5. Web Site Updation and Hosting Policy

a. Official Pages

i. The university’s webmaster is responsible for maintaining the official web site of the university viz., http://www.mdurohtak.ac.in only.

ii. The departments/institutes/centres/offices shall be responsible for the supply of information to UCC in the form of a softcopy accompanied by a hardcopy duly signed by the competent authority for the updation of the university website. The information to be supplied by departments/ institutes/ centres/ offices includes new appointments, promotions, transfers, advertisements, tender notifications published in newspapers, events organised/to be organized, and such other information as may be required to be uploaded on the web site. Such information will be uploaded on the university website by UCC as early as possible.

iii. Departments/Institutes/Centres/Offices/Associations of Teachers/ Employees/ Students are permitted to have pages on MDU’s Intranet Channel of the official Web page.

iv. Official Web pages must conform to the University Web Site Creation Guidelines for Website hosting.

b. Personal Pages

The university computer and network infrastructure is a limited resource. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the university by sending a written request to UCC 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 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. Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the university.

c. Affiliated Pages

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

d. Web Pages for e-Learning

i. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

ii. Because majority of student pages will be published on the University's Web for e-Learning, it must reflect the academic mission. It must be carefully ensured that the published material is not misrepresentative in any way by conflicting with official MDU or other Web sites. If a student publishes a fictional Web site or a Web site modelled after an existing institution or corporation, the site must be clearly identified as a class project.

iii. **Content Disclaimer:** The home page of every class-generated site will include the MDU Content Disclaimer (for pages published on the e-Learning information server, the content disclaimer should be generated automatically).

iv. **Class Information:** The home page of every class-generated site will contain the name of the class, the student's name, the date, and a link to the class home page.

v. **Pages Generated by Class Groups:** Pages produced by class groups, if placed on the e-Learning information server, will be placed on the server under the name of the designated group leader.

vi. **Official Pages:** If Web pages developed for e-Learning become the part of the "official" MDU page, they must be removed from the e-Learning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

e. Student Web Pages

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 given under (b) 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 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.

6. Responsibilities of Those Maintaining Web Pages

Departments, Centers, units, and individuals are responsible for maintaining their own Web pages. All Web pages (including personal pages) must adhere to the MDU Web Page design guidelines

Standards and Design Guidelines should be approved by UCC/Committee constituted by the university for this purpose.

7. Policies for Maintaining Web Pages

a. Pages must relate to the University’s mission.

b. Authors of official MDU and affiliated pages (not class-generated or personal) are required to announce their Web presence by sending an announcement to webs@mdurohtak.ac.in. The announcement should include:

1. The URL.

2. A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the MDU Home Page, and, if applicable, contain additional links to the sponsoring organization or department.

8. University Database (of e-Governance) Use Policy

a. This Policy relates to the databases maintained by the university under the university’s e-Governance project. 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.

b. MDU has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

c. **Database Ownership:** Maharshi Dayanand University Rohtak is the data owner of all the data generated in the university.

d. **Custodians of Data:** Individual Centres/Centres or departments generate portions of data that constitute university’s database. They may have custodianship responsibilities for portions of that data.

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

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

i. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.

ii. Data from the University’s Database including data collected by departments or individual faculty and staff, is for internal university purposes only, unless authorised otherwise by competent authority.

iii. One’s role and function define the data resources that will be needed to carry out one’s official responsibilities/rights. Through its data access policies, the university makes information and data available based on those responsibilities/rights.

iv. 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 office of the University Registrar.

v. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University. The departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies shall be forwarded to the Office of the University Registrar for response.

vi. At no time information may, 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.

vii. Database users who repackage data for others in their unit must inform the recipients of the above data access issues. Re-packagers are responsible for informing and instructing those to whom they disseminate data from the database.

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

a. Unauthorised modification/deletion of the data items or software components,

b. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorised individuals/ departments,

c. Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

d. Attempt to break security of the database servers. Such data tampering actions by university member or outside members will invite disciplinary/legal action against the offender by the university. If the matter involves illegal action, law enforcement agencies may become involved.

9. IT Infrastructure & Information Security Policy

a. Chief Information Security Officer: Vice-Chancellor will appoint a competent officer as University Security Officer, who will be responsible for security of the critical/confidential information stored on university systems and/or transmitted on university data network. He/she will also be responsible for security of the critical IT infrastructure. He/she will device suitable policy and procedures in this regard, and monitor their implementation.

b. Infrastructure Classification:

i. **Critical Infrastructure:** Critical infrastructure includes datacenter infrastructure (including data/information contained therein) and network backbone (Core switch (s), Zone Switch (s), routers, incoming links from ISPs, fiber cable, etc.). These should be provided highest level of security. Any unauthorised national or international intrusion/hacking will invite disciplinary action/criminal prosecution, if required.

ii. **Essential Infrastructure:** Distribution switches, network cabling used for connecting essential systems, development systems, systems used for e-governance operations, and project systems -systems used for operational purpose for day-today work in different branches/departments. These should be provided essential security. Any unauthorised national or international intrusion/hacking will invite disciplinary action/criminal prosecution, if required.

iii. **Required Infrastructure:** Non critical and non-essential infrastructure such as systems and network in students labs. Any unauthorised intrusion, hacking may lead to serious disciplinary action. Any unauthorised national or international intrusion/hacking will invite disciplinary action/criminal prosecution, if required.

c. **Vendor Management:** Any vendor, handling university information, shall ensure complete confidentiality and security at all levels. They shall not share it with any third party without express written authorization.

d. **Physical Security:** Layered security will be put in place to secure university IT infrastructure.

e. **Data Classification and Retention:** Data will be classified into different categories from security perspective. Handling procedures will be devised to ensure sufficient security/confidentiality for each category. Data will be retained online just for its useful life. After that, it will be archived or destroyed as per need.

f. **Employee Awareness Training:** University employees will undergo IT security awareness training as a part of their induction training. The awareness program will also conducted as refresher programme on regular basis.

g. **Incident Response:** Chief Information Security Officer will have an incident response team comprising of specialist mainly from university staff and train them properly, if required, through external agencies. Proper incident response procedures are to be properly documented.

h. **Risk Management:** Risk for different categories of equipment/ data would be identified and arrangements will be made for avoidance, mitigation, or security to counter the risk.

10. Responsibilities of the UCC

a. Campus Network Backbone Maintenance

UCC will be responsible for administration, maintenance and control of the campus network backbone and its active components.

b. Network Services Maintenance

UCC will be responsible for 24x7 network operation and internet facilities. All network failures and excess utilization should reported to the UCC for problem resolution.

Non-intrusive monitoring of campus network traffic will be conducted by the UCC on routine basis. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, UCC will analyse the net traffic offending actions, identify the equipment, and take preventive actions. A report will be submitted to the higher authorities in case the offences are of very serious nature.

c. Physical Connection of Campus Buildings to Campus Network

i. UCC will be responsible for physical connectivity of the campus buildings to the campus network backbone.

ii. All the buildings should have structured cabling like any other wiring such as electrical and telephone cabling. This should form part of plan layout of the new building.

iii. The Engg. Branch will consult UCC for drawing plan for physical demarcation of network cables and network points inside the building and physical connectivity of the building to the "backbone".

iv. UCC will consult with the stakeholders to ensure that end-user requirements are met while protecting the integrity of the campus network backbone.

v. It is not the policy of the university to actively monitor internet activity on the network. But it, sometimes, becomes necessary to examine such activity when a problem occurs or when the traffic on the university's network need optimization.

d. Network Updation and Expansion

i. UCC will review the existing network facilities every 3-5 years and take necessary action for its updation/expansion.

ii. Following procedures should be followed for network expansion:

a. Cat 6 UTP or latest cables should be used for the internal network cabling.

b. Structured cabling standards should be followed. No loose and dangling UTP cables be drawn to connect to the network.

c. The cables should be properly terminated at both ends following the structured cabling standards.

d. Only managed switches should be used. Such management module should be web-enabled. Using unmanaged switches of more than 16 ports is prohibited.

e. Wireless Local Area Networks

i. Where access through Fiber Optic/UTP cables is not feasible, network connectivity will be provided through wireless technology.

ii. UCC will decide the use of radio spectrum by the departments/ institutes/ centres/ offices prior to implementation of wireless local area networks.

iii. UCC will be responsible for controlling network access to the departments/ institutes/ centres/offices through wireless local area networks either via authentication or MAC/IP address restrictions.

iv. The users shall make a written request to the UCC for providing access to internet through wi fi. Such a request should have the recommendation of the respective Head of the Department/Office. Subsequently, UCC will assign a password to the applicant.

v. UCC shall maintain a proper record of the wi fi users.

f. Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic may be retained until the administrative need for them ends. The logs may, subsequently, be flushed.

g. Global Naming & IP Addressing

UCC will be responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. UCC will monitor the network to ensure that such services are used properly.

h. Filing of Complaints by the Users

i. All network-related complaints will filed with the UCC through e-mail or telephone.

ii. UCC will attend such complaints as early as possible.

iii. UCC will maintain a log of the complaints received and complaints attended.

11. Rebuilding the Computer System

When the service engineers re-format the computer systems and re-install OS and other application software, care shall be taken to assign the same hostname, IP address, network mask and gateway as was assigned before formatting. Further, after installing the OS, all the patches/latest service packs should also be properly installed. In case of anti-virus software, it should be ensured that its latest engine and pattern files are also downloaded from the net. In addition, before re-formatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

12. Preservation of Network Equipment and Accessories

Routers, switches, fiber optic cabling, UTP cabling, connecting inlets to the network, racks, and UPSs, including their batteries that are installed at different locations in the university are the property of the university. UCC will be responsible for their maintenance. Tampering of or/and damage to these items by the department or individual user will invite disciplinary action against/legal prosecution of the offender. Tampering includes, but not limited to, the following:

a. Removal of network inlet box.

b. Removal of fiber/UTP cable

c. Opening the rack and changing the connections of the ports either at jack panel level or switch level

d. Taking away the UPS or batteries from the switch room.

e. Disturbing the existing network infrastructure as a part of renovation of the location without the permission of UCC.

13. Campus Network Services Use Agreement

All the users of the campus network facility shall be deemed to have accepted all the provisions University’s IT policy in letter and spirit. It is, therefore user’s responsibility to make himself/herself well aware of the IT policy. Ignorance of the existence of University IT policy shall not be an excuse for any user’s infractions.

14. Enforcement of Policy

UCC will periodically scans the university network for provisions set forth in the Network Use Policy. Failure to comply will make the user liable for discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.