Draft ICT Policy of Pt. B.D. Sharma University of Health Sciences, Rohtak.

A - Scope of Policy

This policy broadly covers all of the University information technology resources – hardware, software, and content; this includes but is not limited to electronic network, systems, computers, devices, software, data/ information, and all content residing in any of these (referred to as "IT resources").
Computers owned or controlled by the by University, and their users will be covered by the IT Policy and consequently Do's and Don'ts apply to these resources. The systems owned / controlled by others, when connected to University network will be subjected to the Do's and Don'ts detailed in the University IT policy.
This policy applies to all records of the University and to the information in those records, regardless of the form or the location.

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, must comply with the Guidelines. Certain violations of IT policy laid down by the University by any user may result in disciplinary/legal action against the offender. If the matter involves illegal action, law enforcement agencies may become involved. Other rules and regulations of the University shall also be applied in addition to this document wherever applicable.

Information and communications technology is a dynamic field and everyday a new technology is being developed therefore the ICT policy will also be updated and extended as and when required.

B - Policy to expand ICT use:

1. ICT for teaching, research & development Activities.
    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 in the working of teaching departments.
        iii. The University will provide a PC / Laptop to all teachers for discharging their teaching, research and other official responsibilities, as per their entitlement.
        iv. The University will provide internet facility to all the faculty members, UG and PG students and administrative offices.
        v. The University will ensure sufficient number of PCs in computer/ Internet labs of the teaching departments/library for use of students/ research scholars/ teachers of University.
        vi. The University would ensure sufficient bandwidth in teaching departments, administrative offices and hostels for efficient & effective use.
        vii. The University will acquire high-end systems depending on the need of the user/department as and when 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 / deployed.

iii. Web Portal for accessing internal and external e-learning resources will be developed/deployed.
iv. University will use licensed system and open source system whenever feasible.
v. The University-generated / created resources will be placed in public domain for use by the students and public, as decided by the competent authority.

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 collaborative tools /platform will be promoted and exploited.
   b. Suitable resources will be developed/deployed.
   c. Unified Communication Infrastructure will be developed/deployed.
   d. Individual username or password login facility will be developed to secure network access.

C. Standard policies and procedures

1. Procurement Policy:
   a. Purchase procedure and policy of the University will be followed.
   b. Hardware & software with standardized specification will be procured.
   c. Attempt will be made to have as long warranty period as possible. After the expiry of warranty period, all the IT equipments will be maintained by authorised vendor on rate contract basis/AMC. The rate contract/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 according to the user requirements.
   e. For the purpose of asset management, inventory of all ICT products will be made in the central store as well as in the IT department of the University.
   f. Certificates, software licence numbers and other such information of the software/hardware and should be stored safely by the user department in case reinstallation or updation of the software/hardware is required.
   g. 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 licensed software will be used. Use of pirated software is prohibited.
   c. Computer purchases made by IT department, will ensure that such computer systems are pre-loaded with operating system with licences of authenticity of 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 and timely updated. 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. Second user should be created on the computer and the user may preferably uses the second user account rather than administrator account. The computer system should be password protected and the password should be kept secret and safe. When the user is not using the system it should be locked.
h. Any computer system may be checked by the IT department by taking appropriate permissions to prevent misuse of the resources.
i. University, as a policy, encourages user community to go for open source software to be used on their systems wherever possible.
j. Site licences of the software, being cheaper option, should be purchased wherever possible.
k. The IT department will provide technical support top the user departments.

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. The power supply to the UPS and Computer peripherals should be provided directly from the power socket on the wall, not from the extension board.
   b. Only one computer system should be connected to a LAN node/socket on the wall.
   c. No wifi router or other personal equipment is allowed to be used on University's LAN to distribute internet.
   d. The ICT resources should be used for teaching, research, patient care and administrative activities etc.
   e. Installation of software other than that provided in the computer should be done in consultation and permission of the IT department. If the system gets damaged by installation of malicious software the responsibility will be of the user.
   f. Client machines, where potentially damaging software is found to exist, will be liable to be disconnected from the University campus network.
   g. If the client's activity adversely affects the network's performance, such a machine is liable to be disconnected from the University campus network.
   h. 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.
   i. Use of University network and computer resources for personal commercial purposes is strictly prohibited.
   j. Network traffic will be monitored for security and performance reasons. Any unauthorised use of the network will result in disconnection and appropriate action as per rules and regulations.

k. 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.
l. Regulation of web content access will be done.
m. The user should keep the username and password secret. If the password is lost or is stolen the user shall inform the IT department. If there is unauthorised access using any password or username the user shall be held responsible.

4. Web Site Updation and Hosting Policy
   a. Official Pages
      i. IT department is responsible for maintaining the official web sites of the University viz, http://www.uhsr.ac.in and http://www.pgimsrohtak.nic.in only.
      ii. The departments/institutes/centres/offices shall be responsible for supply of information to the IT department in the form of a softcopy accompanied by a hard copy duly signed by the competent authority for updation of the information related to them, on University websites. The information to be supplied by departments/ institutes/ centres/ offices includes change in the staff, UG and PG teaching schedule, announcements of examination or other teaching activities not listed in the teaching schedule, results of internal examinations, achievements or awards acquired by the departments, 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. The information should be provided as hard copy duly signed by the head of department. Softcopy of the same information should also be sent by email to the IT department. Such information will be uploaded on the appropriate website by the IT department as early as possible.
      iii. Departments/ incorporated Institutes/Offices/ Students are permitted to have pages on the official web sites. The content for such pages should be provided by the departments.
      iv. Hosting and domain name of the Official University web sites must be as per the state government.
      v. University shall carry out the security audit of the web site to be hosted.

   b. Department's Pages
      i. Information contained in the department's web page on the pgimsrohtak.nic.in or ushr.ac.in should be checked by the respective department and updated every month. A letter stating the information to be updated or if the information is updated the letter should state that the information on the department's web page has been checked and is updated, should be sent to the IT department every month. Information to be uploaded to the web sites should be sent in hard copy signed by the Head of Department and also a soft copy of the same should be provided by email. The information to be updated/uploaded includes change in the Faculty , UG and PG teaching schedule, announcements of examination or other teaching activities not listed in the teaching schedule, results of internal examinations, achievements or awards acquired by the departments, events organised / to be organized, and such other information as may be required to be uploaded on the web site.
   c. 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. Departments may publish learning materials such as pdf files, learning videos or the links to the sites containing such learning materials.

5. Confidentiality of data

Patient data and other confidential documents shall not be viewed/downloaded/printed by any unauthorized person. Any breach of the confidentiality of the information will attract appropriate action enshrined under the relevant government rules and regulations.

6. University Database Use Policy

a. Data is a vital and sensitive University resource for providing useful information. Its use must be protected even when the data may not be confidential.
b. Database Ownership: Pt. B. D. Sharma University of Health Sciences, Rohtak is the data owner of all the data generated in the University.
c. 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.
d. Data Administrators: Data administration activities may be delegated to some of the officers in that department by the data Custodian.
e. Data handling policy:
    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 access/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.

ix. High end database server will be maintained with proper backup.

7. 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. The user should keep the username and password (for internet and Hospital Information and Management System access) safe and secure. The computer system should be kept locked with password when the user is not using the system. If password is breached the user shall inform the IT department and have the password changed.
   c. Infrastructure Classification:
      i. Critical Infrastructure: Critical infrastructure includes ICT infrastructure (including data/information contained therein) and network backbone (Core switch (s), Zone Switch (s),servers, routers, incoming links from ISPs, fibre 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: Wi Fi Access Points, 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 student's 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 rules of the government/ University.

f. Employee Awareness Training: University employees will undergo IT security awareness training as a part of their induction training. The awareness program will also be 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 IT Department / Vendor.
    a. Campus Network Backbone Maintenance.
        i. IT Department / vendor will be responsible for administration, maintenance and control of the campus network backbone and its active components.
    b. Network Services Maintenance
        i. IT Department/Vendor will be responsible for 24x7 network operation and internet facilities. All network failures and excess utilization should reported to the IT Department for problem resolution. Non-intrusive monitoring of campus network traffic will be conducted by the IT Department on routine basis. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, IT Department 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. IT Department 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 PWD / vendor will consult IT Department 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. IT Department 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. IT Department will review the existing network facilities as per requirement and take necessary action for its updation/expansion.
        ii. Following procedures should be followed for network expansion:
            a. The buildings will be connected by minimum 12 core OFC/ latest OFC.
            b. Cat 6 UTP or latest cables should be used for the internal network cabling. This cable should not be more than 80 meters from L2 switch.
            c. Structured cabling standards should be followed. No loose and dangling
            d. The cables should be properly terminated at both ends following the structured cabling standards.
        iii. Only managed switches should be used. Such management module should be web-enabled.

e. Wireless Local Area Networks
   i. Where access through Fibre Optic/UTP cables is not feasible, network connectivity will be provided through wireless technology.
   ii. IT department will decide the use of radio spectrum by the departments/ institutes/centres/ offices prior to implementation of wireless local area networks.
   iii. IT department 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 IT department for providing access to internet through wi- fi. Such a request should have the recommendation of the respective Head of the Department / Office, subsequently, IT department will provide a password to the applicant.
   v. IT department shall maintain a proper record of the Wi-Fi users.

f. Electronic logs
   i. 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
   i. IT Department will be responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. IT Department 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 IT Department through e-mail or telephone.
   ii. IT Department will attend such complaints as early as possible.
   iii. IT Department will maintain a log of the complaints received and complaints attended.

11. Reformatting 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 backup the data on the hard disk and it will be the responsibility of the user to backup the data on an external device. If the hard disk is replaced the damaged hard disk should be submitted to the IT department. The disk may contain sensitive data and should not be handed over to the outsider without authorization.

12. Preservation of Network Equipment and Accessories

a. Routers, servers ,switches, fibre 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. IT Department 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:
   i. Removal of network inlet box.
   ii. Removal of fibre/UTP cable
   iii. Opening the rack and changing the connections of the ports either at jack panel level or switch level
   iv. Taking away the UPS or batteries from the switch room.
   v. Disturbing the existing network infrastructure as a part of renovation of the location without the permission of IT Department.

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

IT Department will periodically scan 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.

15. Rules may be framed for any mishandling, misuse or abuse of IT infrastructure.

16. Rules may also be framed for handling of cases of damage/ theft of IT infrastructure.

17. Jurisdiction: Legal disputes if any of the level of court will be subject to the jurisdiction of Rohtak courts.