The ICFAI University, Dehradun
India

IT Policies & Guidelines
(Date of Release: 25 May 2018)

Prepared by
IT Committee,
The ICFAI University, Dehradun
India

Table of Contents

The ICFAI University, Dehradun IT Policy

Date of Release: 25 May 2020

Version 1.0

Need for IT Policy

This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.

The ICFAI University, Dehradun IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation.

Policies also serve as blueprints that help the institution implement security measures.

An effective security policy is as necessary to a good information security program as a solid foundation to the building.

Hence, The ICFAI University, Dehradun also is proposing to have its own IT Policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of The ICFAI University, Dehradun.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

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

Need for IT Policy

IT Hardware Installation Policy

Software Installation, Backup of Standalone System and Non-Usage of pirated software Policy

Network (Intranet & Internet) Use

Policy Web Site Hosting Policy

University Database Use

Policy Data Privacy Policy

Disaster Recovery Policy

Power Backup Policy

Procedure of IT Replacement

IT Service Level Agreement

IT Helpdesk

It may be noted that university IT Policy applies to technology administered by the university centrally or by the individual School & departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorised resident or non-resident visitors on their own hardware connected to the university network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Center, Computer Labs, Laboratories, Offices of the university recognised Associations/Unions, or hostels and guest houses, or residences wherever the network facility is provided by the university.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the university IT policy.

Further, all the faculty members, 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 university community member may even result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus Students: UG, PG, Research

Faculty (Adhoc, Permanent and Visiting)

Administrative Staff (Non-Technical / Technical) Higher Authorities and Officers

Guests

Resources

Network Devices wired/ wireless Internet Access

Official Websites, web applications

Official Email services

Data Storage

Mobile/ Desktop / server computing facility Documentation facility (Printers/Scanners) Multimedia Contents

IT Hardware Installation Policy

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. What are End User Computer Systems

Apart from the client PCs used by the users, the university will consider servers not directly administered by INTERNET UNIT, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the INTERNET UNIT, are still considered under this policy as "end-users" computers.

C. Warranty & Annual Maintenance Contract

Computers purchased by the University should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

D. Power Connection to Computers and Peripherals

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

E. Network Cable Connection

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 power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities

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

G. Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written approval of the System Administrator. The IT Cell maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it

comprises building name abbreviation and room No. As and when any deviation (from the list maintained by INTERNET UNIT) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified . When the end user meets the compliance and informs INTERNET UNIT in writing/by email, connection will be restored.

H. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed to Schools / departments / Faculty members/ Technical and Non- technical staff, the IT Cell will attend the complaints related to any maintenance related problems.

I. Noncompliance

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

J. INTERNET UNIT/COMPUTER CENTER Interface

The IT Cell upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The IT Cell will provide guidance as needed for the individual to gain compliance.

Software Installation, Backup of Standalone System and Non-Usage of pirated Software Policy

Any personal laptops / notebook's purchases made by the individual School / departments / projects/ individuals should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the School / department /individual personally responsible for any pirated software installed on the computers located in their School/department/individuals' rooms.

A. Operating System and its Updating

i. **Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week.**

ii. **University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.**

iii. **Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates are being done properly.**

B. Antivirus Software and its updating

i. **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.**

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

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from the System Administrator / IT Cell.

C. Backups of Standalone System

University Data is backed up in a manner sufficient to restore any or all of an Information System in the event of a data loss, according to Recovery Time Objectives and Recovery Point Objectives.

Backups are periodically tested to ensure that backups are sufficient and reliable. Backup systems and media protect the confidentiality, integrity and availability of stored data.

Written procedures are maintained to allow unit personnel to recover data in the event of an emergency.

Individual users should perform regular backups of their vital data. 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 can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on storage devices such as pen drives and hard drives.

RESPONSIBILITIES

The System Administrator is responsible for establishing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), in conjunction with data users and owners, for all University Data collected, stored or maintained by the unit. He should verify that Data used by the unit, but collected, stored or maintained by others, have appropriate backup plans.

The Computer Administrators are responsible for implementing backup systems and processes to ensure that RTO and RPO can be met for all data collected, stored or maintained on unit Information Systems. Computer Administrators document backup system operation and test recovery capability.

D. Noncompliance

THE ICFAI faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons

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

E. INTERNET UNIT/COMPUTER CENTER Interface

INTERNET UNIT upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

F. Non-usage of pirated software

Respect for the intellectual work and property of others is vital to the mission of higher education. This principle applies to works of all authors and publishers in all the media, including the labour and creativity resulting in computer software. It encompasses respect for the right to acknowledgement and the right to determine the form, manner, and terms of publication and distribution. Towards this objective the University actively supports non usage of pirated software and encourages use of both product licensed software and free open software.

Unauthorized copying of software is deemed illegal at the University and may force the university as well as individuals to incur legal liability. The Copyright Law protects software authors and publishers in much the same manner as patent law protects inventors. Unauthorized copying of software, including programs, applications, data bases, and code, deprives developers of fair return for their work, may result in increased prices, may reduce the level of future support and enhancement available to the university, and may inhibit the development of software products.

Unless software has been placed in the public domain, the owner of a copyright holds exclusive right to the reproduction and distribution of his or her work. The purchaser of software generally purchases only a license to use the software on one machine. Most licenses do not permit copying although a licensee may generally make a backup or archival copy. Some institutional licenses permit copying for use on local area networks or on multiple machines, but such uses must be authorized in a license agreement commonly called a site license, which might include a network license or a limited-uselicense.

It is the policy of The ICFAI University, Dehradun that unauthorized copying of computer software will not be tolerated and will attract penalty as per University rules. Such copying is both unethical and illegal. University employees and students making, acquiring, or using unauthorized copies of computer software will be subject to university disciplinary sanctions as well as legal action by the copyright owner. The University will not provide legal indemnification for employees or students whose violation arises out of wilful misconduct.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Communication & Information Services (INTERNET UNIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to INTERNET UNIT.

A. IP Address Allocation

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

As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the IT CELL.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

B. DHCP and Proxy Configuration by Individual School, Departments /Sections/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by IT CELL.

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

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running Network Services on the Servers

Individual Schools /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 IT CELL in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

IT CELL takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

IT CELL will be constrained to disconnect client machines where potentially damaging software is found to exist.

A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.

Network traffic will be monitored for security and for performance reasons at INTERNET UNIT.

Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

D. Dial-up/Broadband Connections

Computer systems that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the university's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

i. **This policy applies, in its entirety, to School, department, or division wireless local area networks. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with IT CELL including Point of Contact information.**

ii. **School, departments, or divisions must inform IT CELL for the use of radio spectrum, prior to implementation of wireless local area networks.**

iii. **School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.**

iv. **If individual School wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Co-ordinator, ITCELL.**

F. Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, School / department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to INTERNET UNIT.

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

Web Site Hosting Policy

A. Official Pages

Schools, departments, and Associations of Teachers/Employees/Students may have pages/blogs on THE ICFAI's Intranet Channel of the official Web page. Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting.

As on date, the university's website incharge is responsible for maintaining the official web site of the university viz.,WEBSITE… only.

B. Personal Pages

The university computer and network infrastructure are a limited resource owned by the university. It is recognized that each individual faculty member 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 INTERNET UNIT giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the university. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

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. Web Pages for Student Information Management System(SIMS) / eLearning

The university provide facility for eLearning of Teaching/Learning process. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the LMS, linked through the appropriate department's pages.

Because majority of student pages will also be linked on the University's Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official The ICFAI University, Dehradun or other Web sites.

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

E. Policies for Maintaining Web Pages

Pages must relate to the University's mission and will be maintained and updated periodically by the website in charge. The University Community members should email their request to the Website in charge.

Authors of official THE ICFAI and affiliated pages are required to announce their Web presence by sending an announcement to website incharge.

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 The ICFAI Home Page and, if applicable, contain additional links to the sponsoring School, organization or department.

University Database Use Policy

This Policy relates to the databases maintained by the university administration under the university's eGovernance.
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.
THE ICFAI University 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.

A. Database Ownership: The ICFAI University, Dehradun is the data owner of all the University's institutional data generated in the university.

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

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

D. MIS Data: In course of time as the University generates its SIMS data, the same will be governed by the general guidelines of data privacy and ownership applicable at THE ICFAI.

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

1. **The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.**
2. **Data from the University's Database including data collected by Schools / departments or individual faculty and staff, is for internal university purposes only.**
3. **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.**
4. **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.**
5. **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.**
6. **At no time any information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.**
7. **All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the IQAC, Registrar, Controller of Examinations and Finance officer of the University.**

8. **Database users who repackage data for others in their unit must inform the recipients of the above data access issues.**
9. **Tampering of the database by the School / department or individual user comes under violation of IT policy. Tampering includes, but not limited to:**
    - **Modifying/deleting the data items or software components by using illegal access methods.**
    - **Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.**
        - **Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.**
    - **Trying to break security of the Database servers.**

Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities.
If the matter involves illegal action, law enforcement agencies may become involved.

Data Privacy Policy

A. Overview

The The ICFAI University, Dehradun is committed to the responsible use of personal information and sensitive information collected from and about its students, faculty, staff, business partners and others who provide such information to the university. This commitment is in accordance with both state and national regulations concerning the use of sensitive information. Such sensitive information includes information that could be used to cause financial harm or reputational harm to any individual. This policy applies to personally identifiable sensitive information and how it is collected.

B. Objective

The purpose of this policy is to protect the privacy of individuals who have sensitive information stored (either in electronic or paper form) on assets owned by The ICFAI University, Dehradun, while at the same time providing the University the ability to share this information with authorized entities as required by legitimate academic or business need or by law.

C. Scope

The The ICFAI University, Dehradun Privacy Policy applies to all faculty, staff, students, affiliates, and third-party service providers. This policy is not intended to replace or supersede other existing University policies and procedures relating to the use of maintenance of sensitive information.

D. Privacy Policy

The responsible use of sensitive information requires that the University respects individual privacy, protects against unauthorized access to or use of information, and complies fully with all laws and government regulations in the collection, use, storage, display, distribution and disposal of such information. Authorized uses of sensitive information within the University are limited to uses which a) are necessary to meet legal and regulatory requirements; b) facilitate access to services, transactions, facilities and information; or c) support efficient academic and administrativeprocesses.

Access to sensitive information is limited to:

- **the individual whose information is produced or displayed**

a University official or agent of the University with authorized access based upon a legitimate academic or business interest and a need to know;

an organization or person authorized by the individual to receive the information;

a legally authorized government entity or representative

other circumstances in which the University is legally compelled to provide access to information

or other individuals or entities, as allowed by law, for purposes judged to be appropriate or necessary for the reasonable conduct of University business.

Disaster Recovery Policy

A. Purpose

Disaster recovery refers to the criteria and procedures used to guide management and technical staff in the recovery of computing and network facilities as well as data resources operated by the University in the event that a disaster destroys all or part of the facilities.

B. Scope

The Disaster recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the University. Each supported computing platform has a section containing specific recovery procedures.

C. Applicability

The Disaster recovery plan is applicable to all department administrators, and supervisors responsible for managing critical facilities, including server hardware, software, and data.

D. Disaster Risks and Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created.

- Fire
- Flood
- Thunder storms and High Winds Earthquake
- Computer Crime
- Terrorist Actions and Sabotage

E. Backup Procedures

Every system that the University operates is backed up regularly. The backup media for each of these systems is relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes.

F. Regular backup procedures include:

- Server backups will be performed every business night, excluding holidays. Backup process is shown in Figure 1. For backup we use second party or third-party tool. For example, to backup doc or excel file we use copy command and for database we use database backup command.
- Backups performed on Friday will be kept for a month before recycling.
- The last backup of every month will be considered the monthly backup and kept for a year before recycling.
- Monthly backup media* will be stored in a fireproof safe.
- Backups will be performed and monitored by a fulltime IT staff member.
- Media will be inserted routinely every night before leaving work.
- Backup failures will be reported to Head computer Division and action will be taken quickly to fix the problem.
- Backups will always be performed before upgrading or modifying a server.

***Backup media is used for storing data. In The ICFAI University, Dehradun we use External hard drives/Portable hard drives (shown in Figure 2) for backup, because they are easy to use and faster than optical media.**

Figure 1: Backup process

Figure 2: External hard drives/Portable hard drives

G. Backup Site

The ICFAI University, Dehradun, Address http://172.16.0.202 (connected to LAN)

Power Backup Policy

The University initially installed UPS on individual systems. The policy was revised to install and enable an online UPS which now is in operation.

The ICFAI University, Dehradun is also having their power back up (generators) unit rated 110 KVA for enough back up energy around 10 hours for entire load. The generators turned on and all the protected electric loads seamlessly transferred to the backup power system.

Power outages can spell hindrance for an unprepared service facility. University works to ensure that we have access to back up power to continue serving under any condition.

Procedure of IT Replacement

All Items such as computers, laptops, router, switches etc. must be ordered through University Technology Services.

University Technology Services (UTS) is formed for implementing guidelines for replacing computers, laptops & other items on a five (1) year cycle or as per the university fund position or lease agreement.

The inclusive purpose of the program is to ensure that computing resources on campus are up-to-date. The aim of the University Technology Services are as follows:

- **Ensure that all faculty who use computing resources have access to a computer of sufficient capability to support basic computing needs* in fulfilment of their duties**
- **Ensure that appropriate computing resources are available in Schools / departmental computing facilities and university offices**
- **Ensures that computer systems have sufficient capacity and compatibility to meet each department operational needs**
- **Create a centralized budget which affords basic computing needs for university employees**
- **Implement minimum standards for computing resources on campus increasing the supportability of the institution's installed base of equipment**
- **Maintains ongoing compatibility of computer systems and computer applications used in the Department**
- **Streamline the specification, acquisition, and deployment of new equipment and re-deployment or disposal of old equipment**

***Basic Computing Needs include web access, word processing, messaging, Library access, spreadsheet, database application etc. In addition to that the computing resource must meet Research needs. The Research needs must be funded from departmental budgets/research funds.**

These guidelines shall apply to the replacement cycle for all types of computing resources. University Technology Services has authority and is responsible for the acquisition and support of Information Technology (IT) replacements.

IT Service Level Agreement (SLA)

This IT Service Level Agreement (SLA) document details the service standards which will be delivered by The ICFAI University, Dehradun IT Service Desk to the user community. The service standards are identified so as to work closely with the core business values, demands and requirements. Every effort will be made to fulfil present and future needs of the University and to make the IT experience as enjoyable as possible.

The service standards which were identified by the University IT Service Desk to enhance the staff and student experience are given below:

- **Improve overall quality of staff / student IT**
- **experience High level of staff / student support for IT**
- **A formal mobile and responsive Service Desk to the demands of the entire community**
- **Launch of a formal Staff / Student Incident logging facility via Support Portal**
- **Simplify IT processes for the community**
- **Produce Online user guides / quick fixes / training materials / information packs**
- **Improved communication via one-to-one meetings with other Schools, departments, Students and other stakeholders**
- **Information for system wide issues and outages communicated via IT Support Portal, Emails etc.**
- **Logon assistance portal for staff / students to reset password/unlock accounts**

24/7 IT Help Desk

The 24/7 IT Help Desk is our central point of contact for all The ICFAI University, Dehradun services. Everyone can get fast and friendly technical support—including holidays—via email.

List of staff working for IT support

Sr.No	Name	Designation	Email
1	**Mr. Lalit Mohan Khatri**	System Administrator	systemadmin@iudehradun.edu.in
2	**Mr. Divyam**	Assistant System Administrator	systemadmin@iudehradun.edu.in
3	**Dr. Mohit Kumar**	IT Coordinator	itcoordinator@iudehradun.edu.in

RESPONSIBILITIES OF INTERNET UNIT

A. Campus Network Backbone Operations

1. **The campus network backbone and its active components are administered, maintained and controlled by IT CELL.**
2. **IT CELL operates the campus network backbone such that service levels are maintained as required by the University Schools, departments, and Sections served by the campus network backbone within the constraints of operational best practices.**

1. **Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of IT CELL.**
2. **Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of IT CELL. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the IT CELL. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of IT CELL.**
3. **IT CELL will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.**
4. **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.**

C. Network Expansion

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

D. Wireless Local Area Networks

1. **Where access through Fiber Optic/UTP cables is not feasible, in such locations IT CELL considers providing network connection through wireless connectivity.**
2. **IT CELL is authorized to consider the applications of Schools, departments, or Sections for the use of radio spectrum from IT CELL prior to implementation of wireless local area networks.**
3. **IT CELL is authorized to restrict network access to the Schools, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.**

.

E. Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

F. Global Naming & IP Addressing

IT CELL is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. IT CELL monitors the network to ensure that such services are used properly.

G. Providing Net Access IDs and email Accounts

IT CELL provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the university upon receiving the requests from the individuals on prescribed proforma.

H. Network Operation Centre

IT CELL IT is responsible for the operation of a centralized Network Operation Control Centre. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilization are reported to the IT CELL technical staff for problem resolution.

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the IT CELL. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, IT CELL will analyse the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

IT CELL is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

J. Receiving Complaints

IT CELL may receive complaints from University Community members, if any of the network related problems are noticed by them during the course of attending the end-user computer systems related complaints. Such complaints should be by email/phone.

IT CELL may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call to IT CELL.

The designated person in IT CELL receives complaints from the University Community users and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

IT CELL will be responsible only for solving the network related problems or services related to the network.

L. Disconnect Authorization

IT CELL will be constrained to disconnect any School, department, or section from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a

School, department, or section machine or network, IT CELL endeavours to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, IT CELL provides the conditions that must be met to be reconnected.

Responsibilities of University Computer Centre

A. Acquisition and Maintenance of Computer Hardware & Peripherals

IT CELL is responsible for acquisition and maintenance of the university computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints

IT CELL may receive complaints from University Community members, if any of the particular computer systems are causing network related problems.

IT CELL may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in IT CELL receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. Scope of Service

IT CELL will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

D. Installation of Un-authorised Software

IT CELL or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If IT CELL or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the IT CELL and university authorities.

F. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the IT CELL by University Community Members. After taking necessary corrective action service engineers should inform IT CELL about the same, so that the port can be turned on by them.

G. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

Further, before reformatting 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.

H. Coordination with INTERNET UNIT

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning, COMPUTER CENTER/service engineer may coordinate with INTERNET UNIT staff to resolve the problem with joint effort. This task should not be left to the individual user.

Responsibilities of Schools, Department or Sections

A. User Account

Any School, department, or Section or other entity of the University, can connect to the University network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university. The user account will be provided by IT CELL, upon filling up the prescribed application form and submitting it to IT CELL.

Once a user account is allocated for accessing the university's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the university for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID) to prevent un-authorised use of their user account by others.

As a member of The ICFAI University, Dehradun community, when using the university' network facilities and its user account, it becomes user's duty to respect the University's reputation in all his/her electronic dealings within as well as outside the University.

It is the duty of the user to know the IT policy of the university and follow the guidelines to make proper use of the university's technology and information resources.

B. Logical Demarcation of Department/ Section/Division Networks

In some cases, School, department or Section might have created a internal network with in their premises. In such cases, the School, department, or section assumes responsibility for the network service that is provided on all such internal networks on the School, department or division side of the network backbone. The School, department, or division is also responsible for operating the networks on their side of the network backbone

in a manner that does not negatively impact other network segments that are connected to the network backbone.

Each School, department, or Section should identify at least one person as a Point of Contact and communicate it to IT CELL so that IT CELL can communicate with them directly in case of any network/system related problem at its end.

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

All Schools, Departments, or Sections should provide updated information concerning them periodically (at least once in a month or earlier).

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

Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the webmaster upon receiving the written requests. If such web pages have to be directly added into the official web site of the university,

necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the website in charge.

D. Setting up of Wireless Local Area Networks/Broadband Connectivity

1. **This policy applies, in its entirety, to school, department, or section wireless local area networks/broadband connectivity within the academic complex. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with IT CELL including Point of Contact information.**
2. **Obtaining Broadband connections and using the computers alternatively on the broadband and the university campus-wide network is direct violation of the university's IT Policy, as university. IT Policy does not allow broadband connections within the academic complex.**
3. **School, departments, or Sections must secure permission for the use of radio spectrum from IT CELL prior to implementation of wireless local area networks.**
4. **School, departments, or Sections must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.**
5. **As inter-building wireless networks are also governed by the University IT Policy, setting up of such wireless networks should not be undertaken by the Schools/ departments without prior information to IT CELL.**

E. Security

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

F. Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the university are the property of the university and are maintained by IT CELL. Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

Removal of network inlet box.

Removal of UTP cable from the room.

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

Taking away the UPS or batteries from the switch room.

Disturbing the existing network infrastructure as a part of renovation of the location IT CELL will not take any responsibility of getting them rectified and such tampering may

result in disconnection of the network to that segment or the individual, until the compliance is met.

F. Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the university network policy and with prior permission from the competent authority and information to IT CELL.
University Network policy requires following procedures to be followed for any network expansions:

All the internal network cabling should be as on date of CAT 6 UTP.

UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.

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

Only managed switches should be used. Such management module should be web enabled. Using unmanaged switches is prohibited under university's IT policy. Managed switches give the facility of managing them through web so that IT CELL can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

As managed switches require IP address allocation, the same can be obtained from IT CELL on request.

G. Structured Cabling as a part of New Buildings

All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan. Engineering Branch may make provisions in their designs for at least one network point in each room. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

H. Campus Network Services Use Agreement

The "Campus Network Services Use Agreement" should be read and complied with by all members of the university who seek network access through the university campus network backbone. This can be found on the Intranet Channel of the university web site. All provisions of this policy are considered to be a part of the Agreement. Any Section, Department or Division or individual who is using the campus network facility, is considered to be accepting the university IT policy. It is user's responsibility to be aware of the University IT policy. Ignorance of existence of university IT policy is not an excuse for any user's infractions.

I. Enforcement

IT CELL periodically scans the University network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

Responsibilities of the Administrative Units

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

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

- **Information about New Appointments/Promotions.**
- **Information about Superannuation / Termination of Services. Information of New Enrolments.**
- **Information on Expiry of Studentship/Removal of Names from the Rolls.**
- **Any action by the university authorities that makes individual ineligible for using the university's network facilities.**
- **Information on Important Events/Developments/Achievements.**
- **Information on different Rules, Procedures and Facilities Information related items nos. A through E should reach In-charge IT CELL and Information related items nos. F and G should reach website in charge well in-time.**

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

Guidelines on Computer Naming Conventions

1. **In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network. All computer names on the campus network must use the University standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of IT CELL.**
2. **All the computers should follow the standard naming convention**

Guidelines for running Application or Information Servers

Running Application or Information Servers School/Departments/Section may run an application or information server.

ii Individual faculty, staff or students on the THE ICFAI campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the THE ICFAI network.

Responsibilities for Those Running Application or Information Servers
Schools/Departments/Sections may run an application or information server. They are responsible for maintaining their own servers.

1) Application or information server content and services must follow content guidelines as described in THE ICFAI Guidelines for Web Presence.

2) Obtain an IP address from IT CELL to be used on the server

3) Get the hostname of the server entered in the DNS server for IP Address resolution. University IT Policy's naming convention should be followed while giving the hostnames.

4) Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.

5) Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.

6) Operating System and the other security software should be periodically updated.

7) Sections/Departments may run an application or information server provided they do the following:

I. Provide their own computer, software and support staff

II. Provide prior information in writing to IT CELL on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization web server, contact the IT CELL.

Guidelines for hosting Web pages on the Internet/Intranet

Mandatory

1. Provide the full Internet e-mail address of the Web page maintainer.

2. Provide a link to the THE ICFAI home page from the parent (School/department of origin) home page.

3 Provide a link to the parent home page ("Return to department's home page") on all supporting local pages.

4. Maintain up to date pages. Proof read pages and test links before putting them on the Web, and regularly test and update links.

5. Know the function of HTML tags and use them appropriately.

6 Make provision for providing information without images as printer-friendly versions of the important web pages.

Recommended:

1. Provide information on timeliness (for example: August 2017; updated weekly; updated monthly, etc.)..

2 Provide a section indicating "What's New."

3. Provide a caution statement if link will lead to large pages or images.

4. Indicate restricted access where appropriate.

5. Avoid browser-specific terminology.

6. Provide link text that is clear without the link saying 'click here' whenever hyperlinks are used.

7 Maintain visual consistency across related pages.

8. Provide a copyright statement (if and when appropriate).

9. Keep home pages short and simple.

10. Avoid using large graphics or too many graphics on a single page.

11. Provide navigational aids useful to your users (Link to Home, Table of Contents, Next Page, etc.).

12. Maintain links to mentioned pages.

13. Make your Web pages easy to maintain for yourself and anyone who might maintain them in the future.

14. Avoid active links to pages that are in development. Place test or draft pages in your "test," "temp," or "old" subdirectory. Remember that nothing is private on the Internet: unlinked pages in your directory may be visible.

15 Check your finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended that you check your page with a Web validation service.

16. Think of your users--test with primary user groups (which will be mix of users linking through our high-speed network, and users linking via much slower modems).

17 Conform to accepted, standard HTML codes.

Guidelines for Desktop Users

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

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

1. All desktop computers should have the latest version of antivirus such as Symantec Anti Virus (PC) or Quick Heal and should retain the setting that schedules regular updates of virus definitions from the central server.

2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine.

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

3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.

4. The password should be difficult to break. Password, defined as:

i. must be minimum of 6-8 characters in length

ii. must include punctuation such as ! $ % & * , . ? + - =

iii. must start and end with letters

iv. must not include the characters # @ ' " `

v. must be new, not used before

vi. Avoid using your own name, or names of your wife or children, or name of your School/department, or room No. etc.

vii. passwords should be changed periodically and also when suspected that it is known to others.

viii. Never use 'NOPASS' as your password

ix. Do not leave password blank and

x. Make it a point to change default passwords given by the software at the time of installation

5. The password for the user login should follow the same parameters outlined above.

6. The guest account should be disabled.

7. New machines with Windows XP should activate the built-in firewall.

8. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).

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

10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

11. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

12. In addition to the above suggestions, IT CELL recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise.

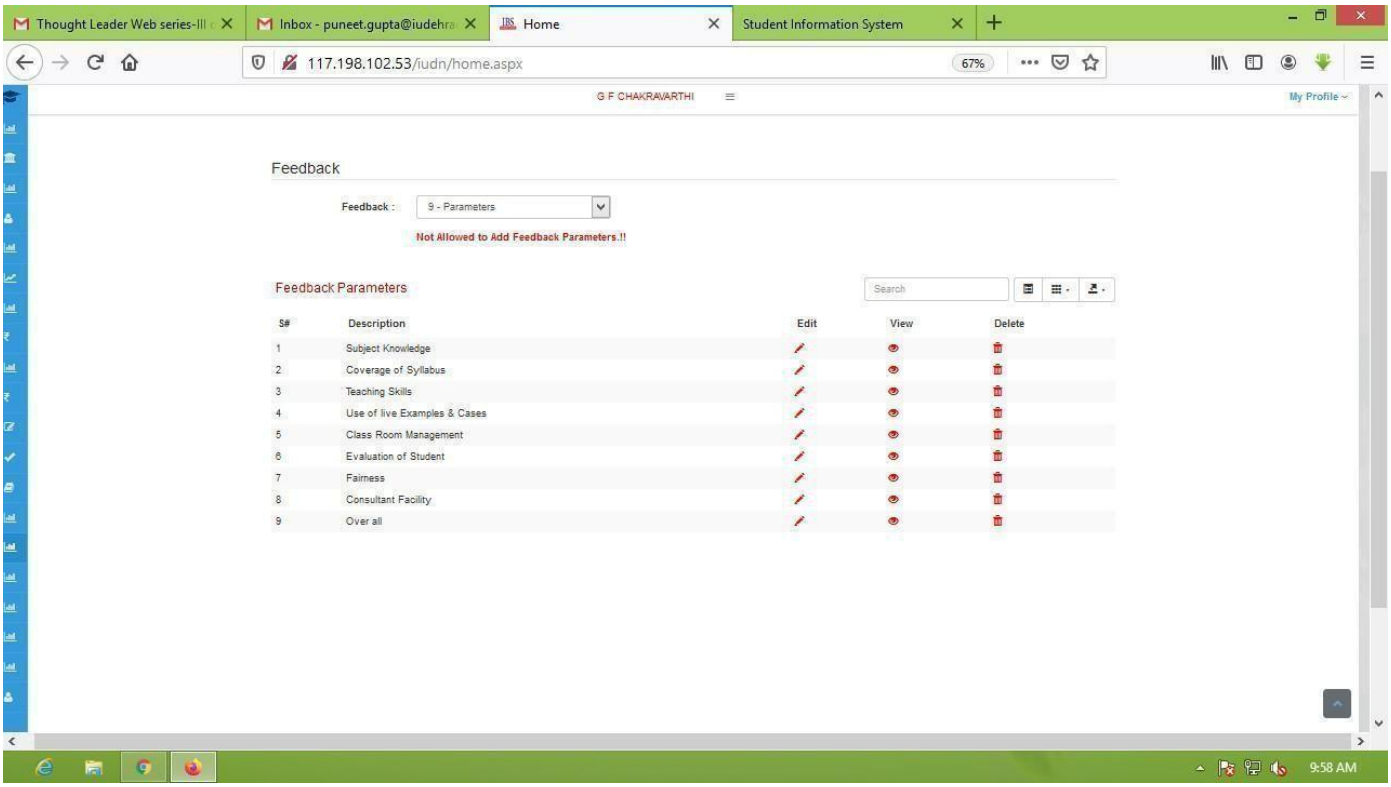
Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

13. If a machine is compromised, IT CELL will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.

14. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, IT CELL technical personnel can scan the servers for vulnerabilities upon request.

Student Information Management System (SIMS)

Feedback Form



*

Appendix II

Online Admission Form

ICFAI UNIVERSITY

Online Application Form

The ICFAI University, Dehradun

Campus-based Programs 2020

Admissions Office:
The ICFAI University Dehradun,
Rajawala Road,
Central Hope Town, Selaqui,
Dehradun - 248197, Uttarakhand. Toll Free number: 1800-599-0767 Email : admissions@iudehradun.edu.in
website : www.iudehradun.edu.in

1. PLEASE SELECT THE PROGRAM YOU WISH TO ENROLL

--Select--

2. NAME OF THE CANDIDATE [As it appears in the School certificates]

Prefix : Mr

Name :
(As it appears in the School Certificates)

Choose File No file chosen

Please upload your recent color Photograph (JPG / GIF format only)
(size 3.5 cm X 4.5 cm)
(File size not more than 25-30 KB)

3. PERSONAL DETAILS

Date of Birth : Day Month Year

Mobile :

E-mail :

Tel (Res) : STD No. Number

Parent Name :

Address :

City : [select city]

State/UT : [select state]

Pin :

Aadhaar No. :

4. ACADEMIC RECORD: SCHOOL/ COLLEGE

a. Class	Name of the School/College	City	Board */ University	Group**	Medium of Instruction	Year of Passing	% of Marks
10							
10+2							
Graduation							
Diploma /							

PG/ Others							

* Indicate State Board/CBSE/ICSE etc.,
** Indicate PCM/Accounts/Commerce etc or Degree or branch of Diploma as applicable.

b. Name & Address of Institute last attended :

City : [select city]

State/UT : [select state]

Pin :

5. DOMICILE STATUS

○ Domicile of Uttarakhand* ○ Non - Domicile

* If you are a Domicile student of Uttarakhand, a certificate from the appropriate authority must be enclosed.

6. Category

○ SC ○ ST ○ OBC ○ General ○ Physically Handicapped ○ Others

7. SOURCE OF CONTACT

○ News Paper Article ○ News paper/Magazine ■ Social Media ■ Website ■ FM/TV
○ Education Fairs ■ advertisements ■ Friends Events of IUD ■ Alumni/Students ○ Marketing Officer
○ Faculty ○ Others

8. AWARDS AND RECOGNITIONS IN ACADEMICS AND SPORTS

List awards, distinctions, honors and scholarships (academic, extracurricular, community services, etc).

Awards	Year	Basis

9. FAMILY BACKGROUND

a. No. of Brothers : **No. of Sisters :**

b. Did any of them studied at IUD or any ICFAI Institute: ■ Yes ■ No

b. Parents Info

Father		Mother	
Name		Name	
Qualifications	Select	Qualifications	Select

Annual Salary/ Income		**Annual Salary/ Income**	

10 . MODE OF PAYMENT

Payment Mode : Select Mode

11. DECLARATION

I hereby declare that the above mentioned information is true to the best of my knowledge and belief.

☐ I Agree

Submit Reset