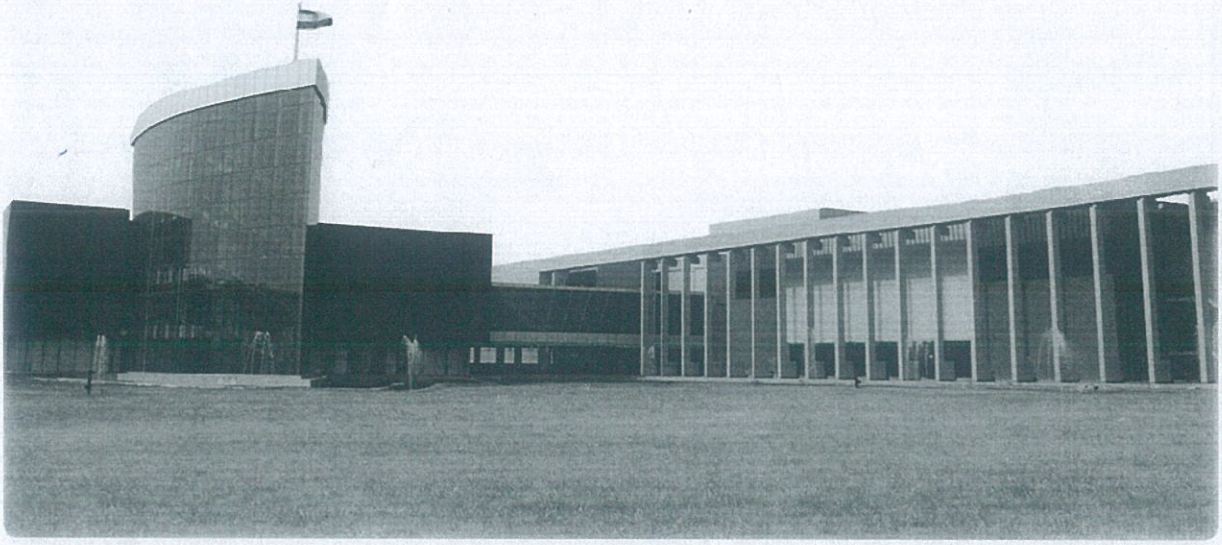
NIFTEM
KNOWLEDGE • INNOVATION • OUTREACH

Information & Communication Technology Policies and Guidelines



Prepared by:
Sh. Nirdesh Kumar Sharma, AR (IT)-Incharge
Er. Kumar Rahul, Assistant Professor- Member
Er. Thangalakshmi, Assistant Professor- Member
Er. Sagar Goel, Network Administrator- Member
Sh. Naveen Kumar, System Administrator- Member

Submitted

Version- 1

INDEX

S. No.	Topic (s)	Page No
1.	Objective of the ICT Policy	
1.1	Principle	
1.2	Mission	
2.	ICT Infrastructure Layout	
3.	Fair / Ethical usage Guidelines	
4.	Scope of ICT policy	
4.1	Hardware	
4.2	Software	
4.3	User	
5.	Information Security Policy	
5.1	Definition of Critical Information	
5.1.1	Restricted Information	
5.1.2	Private Information	
5.1.3	Public Information	
5.2	Statement of responsibility	
5.3	Internet Gateway Security	
5.4	Security / Protection Software	
5.5	Physical security of Servers, Desktop, Laptop, Network Devices etc.	
5.6	Usernames for staff and University associates	
5.7	Maintenance/up-gradation policy	
5.8	Sharing of hardware resources like Desktops, Printers, Scanners etc. by employees & students.	
6	Bandwidth Management	
7	Network Management	
8	USE of Email	
8.1	Limitations in relation to Electronic Mail	
8.2	Limitation on Message and Attachment Size	
8.3	Appropriate Use of Electronic Messaging Services	
9	Do's & Don't	
10	ICT Infrastructure Access Agreement	

3. FAIR / ETHICAL USAGE

a) All users are expected to make use of the ICT resources accessible to them with sensibility and awareness.

b) The NIFTEM - Intranet and Internet access will not be used for commercial activity, personal advertisement, solicitations, or promotions, such as hosting or providing links of commercial websites or email broadcasts of commercial promotions to the users.

c) Any part/component of the ICT infrastructure of the university shall not be misused for Anti-University, Anti-State or Anti-Government activities.

d) The ICT Policy Implementation Committee will be authorized to undertake appropriate measures to ensure maintenance of such discipline and initiate suitable actions for prevention of such undesirable activities.

e) The downloading of text, audio and video files is to be done strictly for official, study & research purposes.

f) Each user must preserve & maintain the confidentiality of the password used by him/her. No user must try to access the ICT resources using other user's password, either knowingly or otherwise.

g) Access to sites that are banned under law or that are offensive or obscene is prohibited. This is also an offence under the Indian IT Act 2000 and attracts severe punishment.

h) Use of the network to tamper with information on other computers, to deliberately spread harmful/pirated programs, compromise other systems, or to cause damage of any kind using the intranet/internet is prohibited, and is an offence under the Indian IT Act 2000. The user is liable for any civil losses caused, in addition to criminal prosecution under the Indian IT Act 2000.

i) No equipment/user other than those registered with the University, cannot be connect to the intranet/Internet without permission of IT.

j) Do not use any device such as podium, mike, projector, biometric; Sound System, CCTV Camera, Wireless etc without permission, if any IT equipment got damaged then a fine (equivalent to the cost of equipment) will impose on student with warning letter for future.

k) A fine of Rs. 500 will be imposed on user(s) if network cable/network box found lost/damaged.

l) A fine of Rs. 500 will be imposed if ID card has been lost.

m) Do not share university username and password outside university.

n) Do not fill wrong information on university ERP Academic Software (iCampus).

o) Do not try to open blocked website, torrent etc, if any genuine website has blocked then contact to IT support for opening of such website. An appropriate action will be taken by ICT implementation committee in case of violation of guideline.

p) Damage of any IT device/equipment/facility by student will impose fine equivalent to the cost of device/equipment/facility.

4. SCOPE OF ICT POLICY

4.1 HARDWARE

Hardware comprises of various items that are used by the end users as well as the items that are used to support the use of ICT by the end users. For example, Servers, Desktops, Laptops, Tablets, Mobile Phones, Printers, Scanners, UPSs, Network Switches, Access Points etc. and various other equipment.

4.2 SOFTWARE

Systems Software comprises of software that make the system function and constitute an integral part of the system. For example, Operating System is a System Software and common applications like E-Mail Client can be considered to be an Application Software.

System Software are proprietary e.g. Windows OR in Public Domain e.g. Linux. Application Software include MS-Office, MS Outlook etc. are proprietary whereas Thunderbird E-Mail, Open Office Suite etc. are Open Source Software.

As far as it is practicable and consistent with the intended purpose, Users ought to prefer Public Domain Software which is available either free OR at a much lower cost.

Software for Common Usage should be identified and implemented across the university in order to achieve consistency of formats and ease of sharing common data.

4.3 USER

Here “user” identifies the full and part-time staff members, students, research scholars, consultants, temporaries, interns, retirees, and other users affiliated with third parties who access university technology resources, all users of ICT equipment owned or leased by the University, all equipment connected to University data and voice networks etc.

5. INFORMATION SECURITY POLICY

5.1 DEFINITION OF CRITICAL INFORMATION

Critical Information Classification is the classification of information based on its level of sensitivity and the impact to the University should that information be disclosed, altered or destroyed without authorization. The classification of information helps determine what basic security controls are appropriate for safeguarding that information. All institutional information should be classified into one of three sensitivity levels, or classifications:

- **RESTRICTED INFORMATION**, (*which is highly valuable and sensitive*). The unauthorized alteration, disclosure or loss of this information can cause significant damage (devastating) to the university, for example, examination results under process, accounts etc. This information must be highly protected as it cannot be easily recovered or brought to its original state easily.

- **PRIVATE INFORMATION**, (*which is of moderate importance and sensitivity*). Its unauthorized alteration, disclosure or loss of this information can cause moderate damage to the university. Generally, the information which is not classified in other two classes falls under this. Reasonable and effective security is required for this information, as recovery of its original state may take sizable amount of resources.

- **PUBLIC INFORMATION**, (*which is of low importance and sensitivity*). Its unauthorized alteration, disclosure or loss of this information can cause little damage to the university. Public information includes press releases, circulars, notifications, course information and research publications, published results on website etc. While little or no controls are required to protect the confidentiality of Public information, some level of control is required to prevent unauthorized modification or destruction of Public information.

All information created, processed, generated, maintained and deleted by the university must be classified into these categories and different levels of user privileges must be defined for each function. Only authorized users can get access to the category of information he/she is authorized to access.

5.2 STATEMENT OF RESPONSIBILITY

- IT Dept. is responsible to facilitate guidance, support and training to user departments in managing their backup of data.

- IT Department having scope to provide a network based storage solution like NAS to automatically obtain backup of their Central Repository including restricted/private information.
- It is the ultimate responsibility of the user / user department to manage the backup of their data.

5.3 INTERNET GATEWAY SECURITY

Securing Internet Gateway is a very challenging task. IT Department is solely responsible to ensure effective security of the gateway. Enterprise Firewall or Unified Threat Management Solution must be implemented effectively with strong policy definitions in line with ICT policy of the university. University Administration must provide an active administrative support to secure the internet gateway by the IT Department.

5.4 SECURITY / PROTECTION SOFTWARE

- The IT department is responsible for installation and maintenance of proper Anti-virus or Internet/Endpoint Security/Protection Software or any other security software as prescribed by the ICT infrastructure Management Committee.
- In case of detection of any issues in the security, the compromised computer/equipment must be disconnected from the NIFTEM Network failing which IT Department shall disable the respective network connection.
- Strict action may be taken by the IT against users who deliberately prevent installation of such security software OR disable such software OR prevent them from running.

5.5 PHYSICAL SECURITY OF SERVERS, DESKTOP, LAPTOP, NETWORK DEVICES ETC.

- The user department where the ICT equipment is installed and used, either temporarily or permanently is responsible for the physical security of it.
- It is responsible for allowing the physical access to the ICT resources only to authorized users.
- It is also responsible to ensure proper power supply with effective grounding (earthing), as well as cleanliness of the equipment and environment including air-conditioning machines.
- The electrical department must ensure proper load on electricity wire/switch before installing additional ICT equipment or other allied equipment like air-conditioning machines etc. The electrical department must get the power load on electricity wire/switch checked every year. The power load on electricity wire/switch must be calculated and increased taking into account requirements of next 2-3 years.

- Users of a user department can access the network via desktop, laptop mobile etc on the campus network. Users are responsible and accountable for the usage of the systems allocated to them.

- Users must take adequate & appropriate measures to prevent misuse of network from computer, Laptop & mobile etc systems that they are responsible for.

- Individual users should take reasonable care of the vulnerability of systems attached to the campus network. In particular, users must apply appropriate service packs, browser updates and antivirus and client security solutions in their MS Windows machines, and necessary upgrades, OS patches, browser updates etc. for other systems.

- If a user department wishes to set up its own Internet access facility, then it should be done under support and monitoring of the IT Department and ensure that deploying such an access facility does not jeopardize the security of the campus network. The user department must completely adhere to the provisions of this ICT Policy for such facility.

5.6 USERNAMES FOR STUDENT, STAFF AND UNIVERSITY ASSOCIATES

A unique username and password are automatically issued to each staff, student, and each University Associate as part of University processes basis on the recommendation of head of respective department.

The Students are authorized to simultaneously use 2 devices for internet access, Faculty & Senior officials are authorized to simultaneously use 5 devices for internet access and lower staffs are authorized to simultaneously use 2 devices for internet access. The university associate(s) is/are authorized to simultaneously use 1 device for internet access

5.7 MAINTENANCE/UPGRADATION POLICY

- On procurement & installation of any new ICT device/equipment, IT department must allocate a unique stock/Asset register number (Asset Identification Number) in the stock/Asset Register. The same number must be written on the device/equipment, which can be used for physical verification. The same must be appropriately updated while transferring out OR disposing/writing off such assets.

- IT department must be vigilant about warranty checks and must take appropriate action if the performance of the device/equipment deviates from the expected performance.

- After the completion of the warranty period, User Department may implement the Annual Maintenance Contract (AMC) for the device/equipment depending on the criticality of its usage, with the approval of the ICT Infrastructure and Management Committee & following the standard procedure laid down by the university from time to time.

- The ICT Infrastructure and Management committee shall define, review, revise, approve and circulate/publish the guidelines & procedure for up-gradation of outdated ICT devices/equipment/components or to improve the performance of existing ICT devices/equipment/components and software. The up-gradation of devices/equipment can be through increasing the performance capacity by adding/replacing some components, like memory, HDD, Graphic card etc. or by replacing the whole device/equipment through a buy-back mechanism depending on the specifications and performance parameters of the device/equipment..

- Necessary budget provisions must be made by the respective user departments for the maintenance and up-gradation of its ICT equipment and software.

5.8 SHARING OF HARDWARE RESOURCES BY EMPLOYEES & STUDENTS

- ICT resources are limited and users are more. Hence, the resources have to be shared sensibly and effectively.

- Use of network office equipment like Network Printers and Photocopier should be encouraged.

- Due care should be taken not to overwrite / delete other users' data on shared resources. In case of any difficulty, guidance and support can be taken from the IT Department.

6. BANDWIDTH MANAGEMENT

Network Management is one of the core functions of the IT Department. University has 1Gbps internet bandwidth through NKN. Distribution of the bandwidth across the campus-LAN is a very important aspect of bandwidth management. The bandwidth management should give priority to Academic, Research contents, Application Software, Services implemented by the university, Research projects, University Website & E-mail facility etc. over general internet browsing and other utilities.

After deep analysis, ICT Policy Implementation Committee has recommended the following bandwidth quota for proper management of internet bandwidth by the various users:

S. No.	Type of User	Quota Limit	Remark
1	Student – B. Tech	**4 GB**	Weekly
2	Student – M. Tech	**6 GB**	Weekly
3	Student – MBA	**6 GB**	Weekly
4	Student – PhD	**8 GB**	Weekly
5	Management	**Unlimited**	Weekly
8	Faculty	**Unlimited**	Weekly
9	Guest / University Associate/service providers	**4 GB**	Weekly
10	Support Staff	**4 GB**	Weekly

15 days before examination start, the internet quota limit for students will be unlimited and again weekly quota policy starts immediately after examination over. The quota limits may be increase or decrease by university.

7. NETWORK MANAGEMENT

The NIFTEM network consists of about 1500 nodes connected through UTP structured cabling with a layered architecture of L3, L2 and EDGE switches with an optical fiber cable as backbone across the campus. ICT Department is the nodal responsible for establishment, maintenance and management of the campus network All the Technical aspects of network related activity like, defining specifications of network components, establishment, maintenance and management of wired and wireless, strategic planning for expansion of LAN, management of internet bandwidth and gateway, Network Security Management, implementation and coordination of government sponsored schemes like NKN etc. is the sole responsibility of the IT Department.

- IT Department is responsible for the core NIFTEM network (includes Internet facilities: email, web etc).
- IT Department will provide connectivity to each User Department, to the gigabit backbone, and also the necessary IP addresses, proxies, email relays etc.

- If any node or part of NIFTEM network "misbehaves" and causes problems for any other user department or the entire campus, or disrupts services, IT department will notify the concerned Head and disconnect the node or part of NIFTEM network from the core network until the problem is fixed satisfactorily.

- IT Department will decide which web sites can be accesses through the campus internet and, shall disallow access to other sites and maintain a mechanism suitable to enforce such a purpose under the guidance and supervision of ICT Policy Implementation Committee.

8. USE OF EMAIL

8.1 LIMITATIONS IN RELATION TO ELECTRONIC MAIL

Electronic mail is a public communication medium that uses a store-and-forward mechanism to pass each message through multiple servers owned by other organizations and via many communication links world-wide.

It is subject to misuse by individuals and organizations worldwide, which send large numbers of unsolicited "spam" email messages to many email addresses. As a result, the University cannot guarantee:

- The successful delivery of electronic messages travelling outside the University.
- The confidentiality of information contained in electronic messages travelling outside the University.
- That all "spam" email messages are blocked from entry to the University email system.

8.2 LIMITATION ON MESSAGE AND ATTACHMENT SIZE

Users shall minimize network traffic by reducing the size of large messages and attachments prior to transmission. Large files should be compressed before attaching them to the message to minimize network traffic.

Electronic documents in excess of any mail server's maximum allowable size may automatically be barred from transmission to the intended recipient. Large documents are best made available by sending recipients a link to the document, we transfer; or in some cases, writing it to a CD or DVD and sending it by courier.

8.3 APPROPRIATE USE OF ELECTRONIC MESSAGING SERVICES

Electronic messaging users shall act in a professional and ethical manner. For example, users shall:

- Maintain professional courtesies and considerations in electronic communication.
- Not transmit abusive or defamatory messages.
- Not transmit an electronic message that breaches legislation (such as the Spam Act 2003) or contravenes University policies.
- Not cause interference to other users of electronic messaging services. Examples of interference include transmission of e-mail chain letters, widespread distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same message.
- Not give the impression that they are representing, giving opinion or making statements on behalf of the University, unless authorized to do so.

9. DO'S & DON'T

- You shall not use any account that has been created for another user without authorization, nor shall you attempt to find out the password of another user, access or alter information, services, usernames, or passwords without authorization.

- You shall not attempt to subvert security measures in any way, nor use a false identity when using ICT facilities and services.

- Without the explicit authorization of the IT Department, you shall not possess any tools nor undertake any activities on ICT facilities or services that could result or assist in the violation of any policy, software license or contract. Examples of these prohibited tools include viruses, Trojan horses, worms, password breakers, network packet observers or sniffers or proxy applications.

  Examples of prohibited activities include creating ping floods; spoofing packets; performing denial-of-service attacks; forging routing information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.

- You shall not attempt to adversely interfere with the operation of any of the University's ICT facilities and services. For the purposes of this document, interfering includes willful physical damage, willful destruction of information, willful interruption of normal operations, and accessing restricted areas without the permission of the ICT Department.

- You shall not willfully waste ICT resources. For example, wasting network bandwidth by downloading or sending large amounts of material that is neither work-related nor study-related.

- You shall not use the University's ICT facilities and services to send obscene, offensive, bogus, harassing or illegal messages.

- You shall not use the University's ICT facilities and services for commercial purposes nor publish or circulate information about other organizations via the University's ICT facilities and services, except where these activities clearly support the business or purpose of the University.

- You shall not use the University's ICT facilities and services in a way that breaches any University policy, such as the University Copyright policy.

- You shall not intentionally create, view, transmit, distribute copy or store pornography or objectionable material via University ICT facilities and services unless it can be clearly demonstrated that it is required for teaching, learning, or research purposes.

- You shall not intentionally create, view, transmit, distribute, copy or store any information, data or material that violates legislation. You shall also not give a person under the age of eighteen years of age access to material regarded as restricted by the University (Publications, Films and Computer Games) (e.g. matters of sex, drug misuse or addiction, crime, cruelty, and violence).

- You shall not attempt to conceal or erase the evidence of a breach of University ICT policy. Users must not use the University's ICT Resources to collect, use or disclose personal information in ways that breach the University's Policy.

- Users must respect and protect the privacy of others.

- The University forbids the use of its ICT resources in a manner that constitutes an infringement of copyright. The law permits copying and/or printing only with the permission of the copyright owner, with a few very limited exceptions such as fair use for study or research purposes (this exception itself is subject to numerous provisos and conditions in the Copyright Act).

- Accordingly Users must not download and/or store copyright material, post copyright material to University websites, transfer copyright material to others or burn copyright material to CD ROMs or other storage devices using ICT Resources, unless the copyright material is appropriately licensed.

- Copyright material includes software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s) and video files.

- ICT Resources must not be used to cause embarrassment or loss of reputation to the University.

- The University does not permit the use of its ICT Resources for unauthorized profit making or commercial activities. **Academic staffs are referred to the University's Outside Earnings Policy with regard to the use of University Resources for private professional practice. General staff are referred to the University's Code of Conduct.**

- Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the network. They may only delete and alter data as required by their authorized University activities

    - Note: This does not apply to specially authorized University computing staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.

- Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorized and competent to do so. All faults or suspected faults must be reported to ICT Department.

- ICT Resources must not be used to distribute unsolicited advertising material from organizations having no connection with the University or involvement in its activities.

- University email lists generated for formal University communications must not be used for other than University business.

- Unless via a personally paid account, files may only be accessed or downloaded if they are work or study related. In any case, files may only be downloaded if it is legal to do so and steps have been taken to ensure that the files are free from viruses and other destructive codes.

- Files may only be attached to email messages if the sender believes they are free from viruses and has taken steps to ensure that they do not contain viruses or other destructive code.

- Users must not attempt to gain unauthorized access to any computer service. The use of another person's login, password or any other security device (e.g. Secured ID, digital signature or biometric identification) is not permitted. Nor must Users exploit any vulnerability in systems or (except authorized staff when checking security of systems as part of their duties) use any technology designed to locate such vulnerabilities or circumvent security systems. The matter may also be referred to the police and/or the Independent Commission against Corruption.

- Users must not facilitate or permit the use of the University's ICT Resources by persons not authorized by the University e.g. Users must not set up a wireless relay base station from their University accounts.

- Limited minor and incidental personal use may be allowed, but it is a privilege and must not interfere with the operation of ICT resources, burden the University with incremental costs, interfere with the User's employment or other obligations to the University and is subject to compliance with University policies. Users should be aware that personal use of the University's ICT Resources may result in the University holding personal information about the User and/or others which may then be accessed and used by the University to ensure compliance with this, and other policies.

10. ICT INFRASTRUCTURE ACCESS AGREEMENT

Please Read the following the ICT Policy & Guidelines of the National Institute of Food Technology Entrepreneurship and Management, Kundli CAREFULLY before accepting/rejecting the policy.

WHOM THIS DOCUMENT CONCERNS

All Users of ICT infrastructure (Computers and the Network) at The National Institute of Food Technology Entrepreneurship and Management, Kundli

REASON FOR POLICY

This policy outlines the responsible use of the Information & Communication Technology Infrastructure at The National Institute of Food Technology Entrepreneurship and Management, Kundli

STATEMENT OF POLICY

All users of the ICT facilities of National Institute of Food Technology Entrepreneurship and Management, Kundli will be subject to the following:

ACCEPTABLE USE POLICY

1. **[System Use]** I shall be responsible for all use of this system. In case I own a computer and decide to connect it to NIFTEM network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of "my computer".) In case I do not own a computer but am provided some ICT resources by NIFTEM, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on IT Department or Department machines).

2. **[Network Use]** I will be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections / equipment, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

3. **[Academic/Research Use]** I understand that the ICT infrastructure at NIFTEM is for academic/research use and I shall not use it for any commercial purpose or to host data/network services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per provisions of Indian law.

4. **[Identity]** I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use NIFTEM ICT resources to threaten, intimidate, or harass others.

5. **[Privacy]** I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

6. **[Monitoring]** I understand that the ICT resources provided to me are subject to monitoring, with cause, as determined through consultation with the university, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited ICT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize university to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of NIFTEM network.

7. **[Viruses]** I shall maintain my computer on this network with current Antivirus/Internet Security/Endpoint Protection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, bots, malware and other similar programs.

8. **[File/Data Sharing]** I shall not use the ICT infrastructure to engage in any form of illegal file/data sharing (examples: copyrighted material, obscene material).

9. **[Security]** I understand that I will not take any steps that endanger the physical or logical security of the NIFTEM network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers/communication devices (including wireless) of any kind (examples: web, mail, proxy, router, managed or unmanaged switch, smart phones) that are visible to the world outside the NIFTEM campus. In critical situations, NIFTEM authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of NIFTEM.

10. **[Penalties]** I understand that any use of ICT infrastructure at NIFTEM that constitutes a violation of NIFTEM Regulations or provisions of Indian Cyber Law could result in administrative or disciplinary or legal procedures.

Your access will be automatically suspended/BLOCKED completely, if the ICT Infrastructure Access Policy is not ACCEPTED by you.

Date: **User's Signature**