Yashwantrao Chavan Maharashtra Open University

Dnyan Gangotri , Near Gangapur Dam, Nashik – 422 222

Internet Usage Policy

Disclaimer

The Internet is a constantly growing worldwide network of computers and servers that contain millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. Users are further cautioned that it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Employees and users (herein referred to as "Users," or "User") accessing the Internet do so at their own risk and understand and agree that **Yashwantrao Chavan Maharashtra Open University, Nashik** (herein referred to as "**The University**") is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at **The University** is governed by the following policy:

Permitted Use of Internet and University computer network: The computer network is the property of The University. Users are provided access to the computer network to assist them in the performance of their jobs. All Users have a responsibility to use The University's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action and/or appropriate legal action.

Computer Network Use Limitations

1. **Prohibited Activities :** The University's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the User's or any other employee's job performance; b) have an undue effect on the computer or University network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of the University. Further, at all times users are responsible for the professional, ethical and lawful use of the

computer system. Personal use of the computer is a privilege that may be revoked at any time.

2. Unacceptable behaviour:

Use of University computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate University purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms.
- Misrepresenting oneself or the University;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the University's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of University networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on University systems and applications.

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material, your colleagues on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- revealing confidential information in a personal online posting, upload or transmission - including financial information and information relating to plans, policies, staff and/or internal discussions
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the corporate network

3. **Illegal Copying :** Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the company.

4. **Communication of Trade Secrets :** Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to The University. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties.
5. **Accessing the Internet :** To ensure security, avoid the spread of viruses & malware, and to maintain The University's Internet Usage Policies or Acceptable Use Policies, employees may only access the Internet through a computer attached to The University's network and approved Internet firewall or other security device(s). Bypassing The University's computer network security by accessing the

Internet directly by personal connections such as (but not limited to) Cellular Networks, or proxy avoidance techniques or by any other means is strictly prohibited.

6. **Frivolous Use :** Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups or other social media, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with not related uses of the Internet.

7. **Virus Detection.** Files obtained from sources outside The University, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by outsiders, may contain dangerous computer viruses that may damage The University's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-University sources, without first scanning the material with virus checking software.

8. **No Expectation of Privacy :** Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using the University's computer equipment. The computer network is the property of The University and may be used only for University purposes.

9. **Waiver of privacy rights.** User expressly waives any right of privacy in anything they create, store, post, send or receive using the University's computer equipment or Internet access. User consents to allow University personnel access to and review of all materials created, stored, sent or received by User through any University network or Internet connection.
10. **Monitoring of computer and Internet usage.** The University has the right to monitor and log and archive any and all aspects of its Computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users via Email, IM & Chat & Social Networking.

11. Blocking Sites With Inappropriate Content

The University has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

12. Blocking Sites With Non-productive Content

The University has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing non-work-related content such as (but not limited to) Drug Abuse; Hacking; Illegal or Unethical; Discrimination; Violence; Proxy Avoidance; Plagiarism; Child Abuse; Alternative Beliefs; Adult Materials; Advocacy Organizations; Gambling; Extremist Groups; Nudity and Risqué; Pornography; Tasteless; Weapons; Sexual Content; Sex Education; Alcohol; Tobacco; Lingerie and Swimsuit; Sports; Hunting; War Games; Online Gaming; Freeware and Software Downloads; File Sharing and Offsite Storage; Streaming Media; Peer-to-peer File Sharing; Internet Radio or TV; Internet Telephony; Online Shopping; Malicious Websites; Phishing; SPAM; Advertising; Brokerage and Trading; Web-Based Personal Email; Entertainment; Arts and Culture; Education; Health and Wellness; Job Search; Medicine; News and Media; Social Networking; Political Organizations; Reference; Religion; Travel; Personal Vehicles; Dynamic Content; Folklore; Web Chat; Instant Messaging or IM; Newsgroups and Message Boards; Digital Postcards; Education; Real Estate; Restaurant or Dining; Personal Websites or Blogs; Content Servers; Domain Parking; Personal Privacy; Finance and Banking; Search Engines and Portals; Government and Legal Organizations; Web Hosting; Secure Sites; or Web-based Applications.

Acknowledgement of Understanding

I understand and will abide by this Internet Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Name: _____

Name of School / Department: _____

Signature: _____

Date: _____

Need for IT Policy

- Basically the University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the YCMOU campus.
- This policy establishes University-wide strategies and responsibilities for protecting the **Co**nfidentiality, **I**ntegrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

Networking: The Computer Centre has established Campus Wide Networking in YCMOU campus by connecting all building in campus by Fiber optic cable with Gigabyte backbone capacity. In University Campus there are around 1300 nodes of LAN and more than 50 Active components like Router, Security Switches, L2 and L3 managed Switches.

- The University has got 1 GBPS internet connectivity under NMEICT Project to provide fast internet connection to all users in the University Campus.

The problems related to uncontrolled surfing by the users:

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

.

With the extensive use of the Internet, network performance suffers in three ways:

When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.

When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.

When computer systems are networked, viruses that get into the LAN, through Intranet/ Internet , spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe downloads, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network. They can slow down or even bring the network to a halt.

Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, Internet Unit has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

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, Yashwantrao Chavan Maharashtra Open University , Nashik 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

Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this university.

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.

IT policies may be classified into following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy

Further, the policies will be applicable at two levels :

- End Users Groups (Faculty, Officers and other staff)
- Network Administrators

It may be noted that university IT Policy applies to technology administered by the university centrally or by the individual departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community.

Further, all the faculty, Officers & staff 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 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.

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. **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.

C. **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.

D. **Shifting Computer from One Location to another**

Computer system may be moved from one location to another with prior written intimation to the Computer Centre (Hardware), as Computer Centre maintains a record of computer identification names and corresponding IP address.

E. **Maintenance of Computer Systems provided by the University**

For all the computers that were purchased by the university centrally, University Computer Centre will attend the complaints related to any maintenance related problems.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects 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 department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

1. 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 or so.
2. 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.
3. 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 a being done properly.

B. Antivirus Software and its updating

1. 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.
2. 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 any service-providing agency.

C. Backups of Data

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 CD or other storage devices such as pen drives.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection is governed under the University IT Policy. Problems within the University's network should be reported to Computer Centre.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the Computer Centre. 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 unauthorisedly 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 Computer Centre.

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.

Responsibilities of Computer Center :

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by Computer Centre.

B. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of Computer Centre.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of Computer Centre. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the Computer Centre. 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 Computer Centre.
3. Computer Centre 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 Computer Centre. Every 3 to 5 years, Computer Centre reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by Computer Centre 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 Computer Centre considers providing network connection through wireless connectivity.
2. Computer Centre is authorized to restrict network access to the Sections, 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. IP Addressing

Computer Centre is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing .

A. Maintenance of Computer Hardware & Peripherals

COMPUTER CENTER is responsible for maintenance of the university owned computer systems and peripherals .

B. Receiving Complaints

COMPUTER CENTER may receive complaints from Users , if any of the particular computer systems are causing network related problems. / any of the computer systems or peripherals are having any problems.

C. Scope of Service

COMPUTER CENTER 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

COMPUTER CENTER 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. 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.

Responsibilities of Department or Sections

A. User Account

Any Centre, department, or Section or other entity 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 Computer Centre , upon filling up the prescribed application form and submitting it to Computer Centre.

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. 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 Computer Centre.

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.

C. 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 Computer Centre.

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.

D. 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.. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

E. Campus Network Services Use Agreement

The "Campus Network Services Use Agreement" should be read 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.

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 Computer Centre.
2. All the computers should follow the standard naming convention

Guidelines for Desktop Users

These guidelines are meant for all members of the 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 department, or room No. or house 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.

11. In addition to the above suggestions, Computer Centre 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.

12. If a machine is compromised, Computer Centre 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.

Yashwantrao Chavan Maharashtra Open University

Dnyan Gangotri , Near Gangapur Dam, Nashik – 422 222

Application for IP Address Allocation

1. Name of School / Department : _____
2. Name of the System (Hostname) : _____
3. Information Outlet Number : _____
4. Make of the System : IBM / SAHARA / DELL / HP / WIPRO /OTHER ____
5. Operating System : Windows XP / Windows Vista / Windows 7 / Windows 8 / Windows Server
6. Net Based Application Running on the System : MKCL / Tally / SOUL Library Software _____

   Other: _____

   Browser : IE / Google Chrome / Mozilla Firefox
7. Which Antivirus Software is running : _____

Date : ___/___/_____ Signature of the Applicant

Signature of Director / Head :_____

For Computer Centre use only:

IP address allocated by Computer Centre : _____

Date : _____ Signature (Computer Centre)

Yashwantrao Chavan Maharashtra Open University

Dnyan Gangotri , Near Gangapur Dam, Nashik – 422 222

Application for Net Access ID Allocation

1. Name of School / Department : _____
2. Name of the System (Hostname) : _____
3. Designation : _____
4. Whether the Appointment is Permanent (Yes / No) : _____
   If No , appointment valid up to : Date :_____/____/_____

Declaration : I have read the University's IT & Internet Usage Policies. I undertake to abide by the rule and regulation of the University for the purpose of Internet use.

Date : ___/___/_____ Signature of the Applicant

"Internet access usage is allowed only for official use as per the provision of the Information Technology (IT) Act, 2000 (No. 21 of 2000). The user shall be solely responsible for internet use from his/her login"

Signature of Director / Head :_____

_____

For Computer Centre use only:

IP address allocated by Computer Centre : _____

Date : _____ Signature (Computer Centre)

Acknowledgement of Understanding

I understand and will abide by this IT Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Name: _____

Name of School / Department: _____

Signature: _____

Date: _____