Shri Shikshayatan College's
IT Policies & Guidelines
(Release: November 2009)

Prepared by -
IT Department
Shri Shikshayatan College
11 Lord Sinha Road
Kolkata -700 071

Table of Contents

Contents

Appendices

Need for IT Policy

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions . Realising the importance of these services, SSC took initiative way back in 2005 and established basic network infrastructure in the academic complex of the college. Over the last five years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the college's academic environment. This has prompted the college decision makers to further augment the network facilities within the academic campus.

Now, the college has about 350 network connections covering more than three buildings across the campus. IT Department (ITD) is the department that has been given the responsibility of running the college's Intranet & Internet services. ITD is running the Firewall security, Proxy, DHCP, DNS, Email, Web, Application and Database Servers and managing the network of the college.

SSC is getting its Internet bandwidth from two sources viz., TATA –DIRECT INTERNET and BSNL BROADBAND. Total bandwidth availability from these two sources was 512 Kbps and upto 2 Mbps respectively. Recently, college is planning to take additional 1.5 Mbps from TATA –DIRECT INTERNET.

While educational institutions are providing access to Internet to their faculty, students and staff, they face certain constraints:

☐ Limited Internet bandwidth.
☐ Limited infrastructure like computers, computer laboratories,
☐ Limited financial resources in which faculty, students and staff should be provided with the network facilities, and
☐ Limited technical manpower needed for network management.

On one hand, resources are not easily available for expansion to accommodate the continuous rise in Internet needs, on the other hand uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes nor governance of the college.

At the outset, we need to recognize 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, ITD 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, Shri Shikshayatan College also is proposing to have its own IT Policy that works as guidelines for using the college'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 this college.
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 organization, departments and individuals who are part of college's community to understand how College policy applies to some of the significant areas and to bring conformance with stated policies.
IT policies may be classified into following groups:
☐ IT Hardware Installation Policy
☐ Software Installation and Licensing Policy
☐ Network (Intranet & Internet) Use Policy
☐ E-mail Account Use Policy
☐ Web Site Hosting Policy
☐ College IRP Database Use Policy
Further, the policies will be applicable at two levels:
☐ End Users Groups (Faculty, Students, Senior administrators, Officers and other staff)
☐ Network Administrators

It may be noted that college IT Policy applies to technology administered by the college centrally or by the individual departments, to information services provided by the college administration, or by the individual departments, or by individuals of the college community, or by authorized resident or non-resident visitors on their own hardware connected to the college network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centres, Laboratories, Offices of the college recognized Associations/ Unions, wherever the network facility was provided by the college.
Computers or Laptops 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 college IT policy.
Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the College's information technology infrastructure , must comply with the Guidelines. Certain violations of IT policy laid down by the college by any college member may even result in disciplinary action against the offender by the college authorities. If the matter involves illegal action, law enforcement agencies may become involved.

IT Hardware Installation Policy
College 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 or desk 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 college will consider servers not directly administered by ITD, 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 ITD, are still considered under this policy as "end-users" computers.
C. **Warranty & Annual Maintenance Contract**
Computers purchased by any College/Centre/Department/Project 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 earthing 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 intimation to the ITD, as ITD maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building wing name abbreviation and room no. As and when any deviation (from the list maintained by ITD) 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 ITD in writing/by email, connection will be restored.

H. **Maintenance of Computer Systems provided by the College**

For all the computers that were purchased by the college centrally and distributed, College Computer Maintenance Cell (CCMC) will attend the complaints related to any maintenance related problems.

I. Noncompliance

SSC faculty, staff, 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 affects on other individuals, groups, departments, or even whole college. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

J. ITD/CCMC Interface

ITD 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 CCMC, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The ITD will provide guidance as needed for the individual to gain compliance.

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, College IT policy does not allow any pirated/unauthorized software installation on the college owned computers and the computers connected to the college campus network. In case of any such instances, college 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

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 or so.

ii College 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 a being done properly.

B. Antivirus Software and its updating

i Computer systems used in the college 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 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 foolproof solution. Apart from this, users should keep their valuable data either on Floppy, or CD or other storage devices such as pen drives.

D. Noncompliance

SSC 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 affects on other individuals, groups, departments, or even whole college. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

E. ITD/CCMC Interface

ITD 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 CCMC, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The ITD will provide guidance as needed for the individual to gain compliance.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the College, referred to hereafter as "the

Network", either through an authenticated network access connection is governed under the College IT Policy. The Information and Technology Department (ITD) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the College's network should be reported to ITD.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the college network, should have an IP address assigned by the ITD. 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 unauthorized 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 ITD. 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 Departments /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 college.

Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by ITD. 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 departments/individuals connecting to the college 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 ITD in writing and after meeting the requirements of the college IT policy for running such services. Non-compliance with this policy is a direct violation of the college IT policy, and will result in termination of their connection to the Network. ITD takes no responsibility for the content of machines connected to the Network, regardless of those machines being College or personal property. ITD 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 College'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 College Network connects. College 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 ITD. 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 College's campus-wide network, whether college's property or personal property, should not be used for dial-up/broadband connections, as it violates the college'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 college, department, or division wireless local area networks. In addition to the requirements of this policy, college, departments, or divisions must register each wireless access point with ITD including Point of Contact information.

ii. College departments, or divisions must inform ITD for the use of radio spectrum, prior to implementation of wireless local area networks.

iii. College, 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.

F. Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any department of the college under any research programme/project should ideally be pooled with the college's Internet bandwidth, and be treated as college's common resource. Under particular circumstances, which prevent any such pooling with the college Internet bandwidth, such network should be totally separated from the college's campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the college gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the college 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 ITD.

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

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students and the College's administrators, it is recommended to utilize the college's e-mail services, for formal College communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal College communications are official notices from the College to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general College messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to **http://www.shrishikshyatancollege.org** and click on web mail then with their **User ID** and **password**. For obtaining the college's email account, user may contact ITD for email account and default password by submitting an application in a prescribed proforma. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

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

(2) using the facility for illegal/commercial purposes is a direct violation of the college's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
(3) while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
(4) User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
(5) User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
(6) Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of theiraccount.
(7) User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
(8) User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
(9) While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
(10) Impersonating email account of others will be taken as a serious offence under the college IT security policy.
(11) It is ultimately each individual's responsibility to keep their e-mail account free from violations of college's email usage policy.
(12) Any Spam mail received by the user into INBOX should be deleted and not opened
(13) Any mail wrongly stamped as SPAM mail should be forwarded to
(14) All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.
The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the college's campus network, or by using the resources provided by the college to the individual for official use even from outside.

Web Site Hosting Policy

I. Official Pages

College/Centres, Departments, and Associations of Teachers/Employees/Students may have pages on the official Web page.
Official Web pages must conform to the College Web Site Creation Guidelines for

Web site hosting.
As on date, the college's webmaster is responsible for maintaining the official web site of the college viz., http://www.shrishikshayatancollege.org only.

Personal Pages:

The college computer and network infrastructure is a limited resource owned by the college. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the college by sending a written request to ITD giving the details of the hyperlink of the URL that he/she wants to be added in the official website of the college. 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 college.

II. Web Pages for IRP

Though the college does not have this facility as on this date, this Policy relates to future requirements for Web pages for IRP authored as a result of Teaching/Learning process.

Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages. Because majority of student pages will be published on the College's Web for e-Learning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official SSC or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

The following are the storage and content requirements for class-generated student Web pages:

Servers:

It is recommended that pages be placed on the student information server, but pages developed for classes also may be placed on departmental servers or the main campus server meant for IRP purpose.

Maintenance:

If the pages are published on the IRP information server, they will be maintained under the default rules for personal e-Learning pages. The instructor will maintain pages that are published on departmental servers or the main campus server meant for e-Learning purpose.

Content Disclaimer:

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

Class Information:

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

Servers:

Pages will be placed on the student information server.

Maintenance:
Pages published on the student information server will be maintained under the default rules for personal student pages.
Content Disclaimer:
Every personal page will include the JNU Content Disclaimer (the content disclaimer will be generated automatically):
Responsibilities for Those Maintaining Web Pages
College, Centers, Departments, Units and Individuals are responsible for maintaining their own Web pages.
SSC Web pages (including personal pages) must adhere to the SSC Web Page Standards and Design Guidelines and should be approved by SSC WebPages Advisory Committee.
Policies for Maintaining Web Pages
Pages must relate to the College's mission.
Authors of official SSC and affiliated pages (not class-generated or personal) are required to announce their Web presence by sending an announcement to sscadmin@shrishikshayatancollege.org .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 SSC Home Page and, if applicable, contain additional links to the sponsoring organization or department.
College Database(of e-Governance) Use Policy
This Policy relates to the databases maintained by the college administration under the college's e-Governance.
Data is a vital and important College resource for providing useful information. Its use must be protected even when the data may not be confidential.
SSC 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 college's approach to both the access and use of this college resource.
A. **Database Ownership:** Shri Shikshayatan College is the data owner of all the College's institutional data generated in the college.
B. **Custodians of Data:** Individual Centres or departments generate portions of data that constitute College'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 Components:** For the purpose of eGovernance, Management Information System requirements of the college may broadly be divided into seven categories. These are:
☐MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
☐STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)
☐FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
☐PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
☐PROJECT INFORMATION MONITORING SYSTEM (PIMS)
☐LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
☐DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

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

1) The college's data policies do not allow the distribution of data that is identifiable to a person outside the college.

2) Data from the College's Database including data collected by departments or individual faculty and staff, is for internal college 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 college 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 College Jt. Secretary.

5) Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the College 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 College Registrar for response.

6) At no time may 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 college or its departments.

7) All reports for UGC and other government agencies will be prepared/compiled and submitted by the Registrar of the College/Coordinator (Eval.)

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

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

i. Modifying/deleting the data items or software components by using illegal access methods

ii. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments

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

iv. Trying to break security of the Database servers.

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

RESPONSIBILITIES OF ITD

A. Campus Network Backbone Operations

i. The campus network backbone and its active components are administered, maintained and controlled by ITD.

ii. ITD operates the campus network backbone such that service levels are maintained as required by the College departments and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings' Network

i. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of ITD.
ii. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of ITD. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the ITD. 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 ITD.
iii. ITD will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
iv. It is not the policy of the College 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 College's Internet links.

C. Network Expansion

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

D. Wireless Local Area Networks

i. Where access through Fiber Optic/UTP cables is not feasible, in such locations ITD considers providing network connection through wireless connectivity.
ii. ITD is authorized to consider the applications of College departments, or divisions for the use of radio spectrum from ITD prior to implementation of wireless local area networks.
iii. ITD is authorized to restrict network access to the School, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.
20

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

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

G. Providing Net Access IDs and email Accounts

ITD 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 college upon receiving the requests from the individuals on prescribed proforma.

H. Network Operation Center

ITD is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available in college hours , 6 days a week. All network failures and excess utilization are reported to the ITD technical staff for problem resolution.
Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the ITD. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, ITD will analyze 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

ITD 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

ITD may receive complaints from CCMC, 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.

ITD 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 ITD.

The designated person in ITD receives complaints from the users/CCMC 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

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

L. Disconnect Authorization

ITD will be constrained to disconnect any School, department, or division 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 division machine or network, ITD endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a School, department, or division is disconnected, ITD provides the conditions that must be met to be reconnected.

Responsibilities of College Computer Maintenance Cell (CCMC)

A. Maintenance of Computer Hardware & Peripherals

CCMC is responsible for maintenance of the college owned 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

CCMC may receive complaints from ITD, if any of the particular computer systems are causing network related problems.

CCMC 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 CCMC receives complaints from the users/ITD 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

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

D. Installation of Unauthorised Software

CCMC 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 CCMC or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the college, such incidents should be brought to the notice of the ITD and college 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 CCMC by ITD. After taking necessary corrective action CCMC or service engineers should inform ITD 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 ITD

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, CCMC/service engineer may coordinate with ITD staff to resolve the problem with joint effort. This task should not be left to the individual user.

Responsibilities of School/Centre, or Department

A. User Account

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

Once a user account is allocated for accessing the college's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the college 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 unauthorised use of their user account by others.

As a member of Shri Shikshayatan College community, when using the college' network facilities and its user account, it becomes user's duty to respect the College's reputation in all his/her electronic dealings within as well as outside the College.

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

B. Logical Demarcation of Department/ Division Networks

In some cases, School/Centre, department or Division might have created a internal network with in their premises. In such cases, the School/Centre, department, or division 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/Centre, department, or division should identify at least one person as a Point of Contact and communicate it to ITD and CCMC so that ITD or CCMC can communicate with them directly in case of any network/system related problem at its end.

C. Supply of Information by College/Centre, Department, or Division for Publishing on /updating the SSC Web Site

All Schools/Centres, Departments, or Divisions 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/Centre, Department, or Division level **,** along with a softcopy to be sent to the webmaster operating from ITD. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by College/Centre, Department, or Division.

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 college, 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 Director, ITD well in advance.

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

i. This policy applies, in its entirety, to school, department, or division 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 ITD including Point of Contact information.

ii. Obtaining Broadband connections and using the computers alternatively on the broadband and the college campus-wide network is direct violation of the college's IT Policy, as college IT Policy does not allow broadband connections within the academic complex.

iii. School, departments, or divisions must secure permission for the use of radio spectrum from ITD prior to implementation of wireless local area networks.

iv. 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.

v. As inter-building wireless networks are also governed by the College IT Policy, setting up of such wireless .networks should not be undertaken by the College/Centres without prior information to ITD.

E. Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the College 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 college are the property of the college and are maintained by ITD.

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

i) removal of network inlet box

ii) removal of UTP cable from the room

iii) opening the rack and changing the connections of the ports either at jack panel level or switch level

iv) taking away the UPS or batteries from the switch room.

v) disturbing the existing network infrastructure as a part of renovation of the location

ITD 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.

G. Additions to the Existing Network

Any addition to the existing network done by School/Centre, department or individual user should strictly adhere to the college network policy and with prior permission from the competent authority and information to ITD.

College Network policy requires following procedures to be followed for any network expansions:

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

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

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

iv. Managed and unmanaged switches should be used. Such management module should be web enabled.. Managed switches give the facility of managing them through web so that ITD 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

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

H. 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.

I. Campus Network Services Use Agreement

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

J. Enforcement

ITD periodically scans the College 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

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

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

A. Information about New Appointments/Promotions
B. Information about Superannuation/Termination of Services
C. Information of New Enrolments
D. Information on Expiry of Studentship/Removal of Names from the Rolls
E. Any action by the college authorities that makes n individual ineligible for using the college's network facilities
F. Information on Important Events/Developments/Achievements
G. Information on different Rules, Procedures, Facilities

Information related items nos. A through E should reach Director (ITD) and Information related items nos. F and G should reach webmaster 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 a floppy or CD or by email) should be sent to ITD so as to reach the above designated persons.

Guidelines on Computer Naming Conventions

i 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 following conventions. Computers not following standard naming conventions may be removed from the network at the discretion of ITD.

ii All the computers should follow the following naming convention. The host name should start with the building abbreviated name, followed by the room No and the computer No., if more than one computer is installed in the same room. The abbreviated names of different College/Dept buildings are as given below:

1. Library :SSCLIB
2. Staff Room :SSCSTAFF
3. Office : SSCOFFICE
4. IT : SSCIT

Etc.

Example I: A computer in room No. 213 of Department of Hindi will be named as SSCH213 and its
Workgroup will be SSC.

Servers should either be named after the department and the room they are in. All such departments should inform ITD in writing about such server installations along with a canonical name that gives an indication about the purpose of the server
Example:

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 JNU home page from the parent (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. Proofread 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 2005; 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 JNU Network User Community and users of the College network.

Due to the increase in hacker activity on campus, College 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 AntiVirus (PC) or Norton AntiVirus (Macintosh) or Mcafee or Trend Micro Officescan 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.
12. In addition to the above suggestions, ITD 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, ITD 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, ITD technical personnel can scan the servers for vulnerabilities upon request.
15. It is recommended to run
I. Microsoft basic security Analyzer
II. Microsoft Anti-spyware
III. Malicious Codes Removal Tool
software that are freely down loadable from the Microsoft web site. After downloading them, the first two software need to be installed for making use of them. Microsoft Basic security Analyzer is meant for scanning the Windows based PC for missing service packs/patches, weak passwords, and other vulnerabilities. Anti-spyware is meant for checking if there are any spy ware programs running on your computer system in the background and to delete them. Malicious Code removal tool will scan the computer for certain viruses and removes them.

Concluding Note

As a concluding note, it is explicitly emphasized that though the policies focus on issues related to the technology and information usage, it may be understood that they derive broader meaning and significance from not only fundamental rights but also basic rules and responsibilities that apply to all aspects of the College community. If something is not specified explicitly in the policy or guidelines as illegal or unauthorized, it may still be infraction of the college rules, if it violates the basic rules of the college and responsibilities of the institution and college community. So, it is essential and important to use ones own wisdom and critical thinking in evaluating new situations.

Appendix I

Campus Network Services Use Agreement

Read the following important policies before applying for the user account/email account. By signing the application form for IP address allocation/Net Access ID (user account)/email account, you agree to act in accordance with the IT policies and guidelines of Shri Shikshayatan College. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of the college. User can have a copy of the detailed document from the Internet (viz.,**http://www.shrishikshayatancollege.org/downloads/SSC_ITpolicy.pdf**).
A Net Access ID is the combination of a username and a password whereby you gain access to College computer systems, services, campus networks, and the internet.

I. **Accounts and Passwords**

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the College.

Students, staff and faculty who leave the College will have their Net Access ID and associated files deleted. No User will be allowed more than one Net Access ID at a time, with the exception that faculty or officers who hold more than one portfolio, are entitled to have Net Access ID related to the functions of that portfolio.

II. **Limitations on the use of resources**

On behalf of the College, ITD reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

III. **Computer Ethics and Etiquette**

The User will not attempt to override or break the security of the College computers, networks, or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT Policy violation.

In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

User's Net Access ID gives him/her access to e-mail, and campus computing resources. The use of these resources must comply with College policy and applicable. Electronically available information

(1) may not contain copyrighted material or software unless the permission of the copyright owner has been obtained,

(2) may not violate College policy prohibiting sexual harassment,

(3) may not be used for commercial purposes,

(4) should not appear to represent the College without appropriate permission, or to represent others,

(5) may not appear to represent other organizations or companies,

(6) may not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,

(7) may not contain scripts or code that could cause a security breach or permit use of resources in opposition to College policy, and

(8) WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show date of last revision and an address (e-mail or postal) for correspondence. ITD equipment does not support use of scripting in individual pages.

IV. **Data Backup, Security, and Disclaimer**

ITD or CCMC will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an ITD/CCMC staff member in the process of helping the user in resolving their network/computer related problems. Although ITD/CCMC make a reasonable attempt to

provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, ITD makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold ITD or CCMC, as part of SSC, harmless for any such liability or expenses. SSC retains the right to change and update these policies as required without notification to the User.

V. **Account Termination and Appeal Process**

Accounts on SSC network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources. When an account is terminated or disabled, ITD will make an attempt to contact the user (at the phone number they have on file with ITD) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the ITD of the same But, if the termination of account is on the grounds of willful breach of IT policies of the college by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Director ITD, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Appeals Board duly constituted by the college for this purpose to review the evidence and hear reasons why an appeal should be considered. If the Appeals Board recommends revival of the account, it will be enabled. However, the decision of the Appeals Board is final and should not be contested.

Users may note that the College's Network Security System maintains a history of Infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate College authorities.

Appendix II

INFORMATION TECHNOLOGY DEPARTMENT

Application for IP Address Allocation

S.No. Details To be filled

1. Location of the System Centre / Department : _____
Room No. _____
Floor /Lab.No _____
Occupied by _____
2. Identification Name of the System
(Hostname)
_____
3. IO Box Number _____
4.. Make of the system ACER / Compaq / HCL / IBM / HP / Dell / If Other, Specify
_____
5. MAC / Physical / Adapter address
6. Operating System Win95, Win98, W2K, WinXP, Linux, Solaris, if Other, specify _____
7. Net-based Applications Running on the system

a. Yahoo Messenger
b. MSN Messenger
c. AOL
d. Microsoft Antispyware
e. SPSS
f. Others, specify……..
8 Whether connected directly to the LAN or through another hub / switch YES / NO, If yes ,
a. Directly connected to LAN
b. Through Hub/Switch located in the same room / different room
9. If the system is configured as server , services that are enabled
a. Http h. SMTP
b. FTP i. Sendmail
c. Netfs j. MySql
d. Network k. SMB
e. Nfs l. Telnet
f. POP3, Any other, specify_____
g. IMAP,
10. Whether in general used by single user or many users Single / Many
11. Which Antivirus Software is running
a. Trend Micro
b. MacAfee
c. Norton
d. any other, please specify _____
Date:
Signature of the Applicant

ITD Office Use only
IP address allocated by ITD

Applicant's copy
Signature
on Behalf of ITD
IP address 172.16. . .
Subnet Mask 255.255. .
Gateway 172.16.
DNS Entry 202.41.10.31
202.41.10.32
Host name :
IP address 172.16. . .
Subnet Mask 255.255. .
Gateway 172.16.
DNS Entry 202.41.10.31
202.41.10.32

Appendix III
COMMUNICATION & INFORMATION SERVICES
INFORMATION TECHNOLOGY DEPARTMENT
Application for Net Access ID Allocation
Date:
Signature of the Applicant

ITD Office Use only
Net Access ID allocated by ITD
Applicant's copy
Signature
on Behalf of ITD
S.No. Details To be filled
1. Name of the Applicant Prof./Dr./Mr./Ms./ .....
2. Location School /Centre / Department :
Room No. _____
Contact Telephone No. _____
3. Date of birth ----/----/------
4. Designation _____
5. Whether the appointment is permanent? Yes/No
if No, appointment valid up to : Dt.: / /
Net Access ID allocated
Name of account holder
Account Valid Up to
Net Access ID allocated
Name of account holder
Account Valid Up to

Appendix IV
COMMUNICATION & INFORMATION SERVICES
INFORMATION TECHNOLOGY DEPARTMENT
Application for Network Access Account Allocation for Students
Date:
Signature of the Applicant
Mr./Ms..... is a bonafide student of this School/Centre and the information given
above by him/her is correct as per our records. He/she may be given Net Access ID.
Signature of A.O. of the School

ITD Office Use only
Network Access ID allocated by ITD
Applicant's copy
Signature
on Behalf of ITD
S.No. Details To be filled
1. Name of the Applicant Mr./Ms.....
2. Location : _____
Centre : _____

3. Roll No. _____
4. Programme of Study _____
5. Duration of the course __ Semesters
6. Date of joining the Course __/__/_____
Net Access ID allocated
Name of account holder
Account Valid Up to
Net Access ID allocated
Name of account holder
Account Valid Up to

Appendix V
INFORMATION TECHNOLOGY DEPARTMENT
SHRI SHIKSHAYATAN COLLEGE
REQUISITION FORM FOR E-MAIL ACCOUNT
1. Full Name : _____
2. Designation : _____
3. Dept./Centre : _____
4. Office Telephone :_____
5. Please specify the E-mail Account Name you wish to have
Option One
@shrishikshyatancollege.org
Option two
@ shrishikshyatancollege.org
Date : Signature of the Applicant

User Counterfoil
The following email ID is created for Prof./Dr./Mr./Ms _____
_____
on _____.
@ shrishikshyatancollege.org

Signature
on Behalf of ITD