Name of the Policy/ Guidelines	Information TechnologyPolicy
Short Description	Policy and Guidelines on use of Information Technology in Education and Governance
Scope	This Policy is applicable to all Teaching, Non-Teaching, Staff, Students, Research Scholar and Administrator of the Constituent Units and Departments of Nitte (Deemed to be University)
Policy status	☐Original ☒ Revised
Date of approval of Original Policy	22.04.2015
Revision No.	2
Brief description of last revision	—
Date of approval of current revision	23-12-2019
Effective date	23-12-2019
Approval Authority	Board of Management
Responsible officer	Registrar

INFORMATIONTECHNOLOGY POLICY

Contents

INTRODUCTION

With digitisation pervading into every facet of our life, we are witnessing an unprecedented need for internet. Further, to increase productivity by reducing monotony of duplication, IT enabled services have become indispensable requisites in educational institutions and research organizations. Realizing the importance of these services, NITTE (Deemed to be University) (herein after referred as NitteDU) took the initiative way back in year 2009 to establish basic network infrastructure for the IT department in the academic complex at NitteDU assigning it with the responsibility of running the NitteDU intranet and Internet services.The IT Section manages the firewall security, proxy, DHCP, DNS, E-mail, web and application servers and the network of the NitteDU.

NEED FOR IT POLICY

In the absence of clearly defined IT policies, it is 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.

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

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 policies that govern information, security processes 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.

OBJECTIVES OF THE POLICY

1. To maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the NitteDU on the campus.
2. To outline NitteDU-wide strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by the NitteDU.

SCOPE & JURISDICTION

It may be noted that IT Policy of NitteDU applies to technology administered by the NitteDU centrally or by the individual departments, to information services provided by the NitteDU administration, or by the individual departments, or by individuals of the NitteDU community, or by authorised resident or non-resident visitors on their own hardware connected to the NitteDU network. This IT policy also applies to the resources administered by the central administrative departments such as library, computer centres, laboratories, offices of the NitteDU recognised associations, or hostels and guest houses, or residences wherever the network facility was provided by the NitteDU.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the IT policy of NitteDU. Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the NitteDU information technology infrastructure, must comply with the guidelines. Certain violations of IT policy laid down by the NitteDU by any member may even result

in disciplinary action against the offender by the NitteDU authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

This Policy Applies to all Stake Holders and resources of NitteDU, its Institutes, Units and Hospitals as detailed below:

A. Stake holders coming under the purview of following establishments are covered under this policy

1. NITTE (Deemed to be University)
2. A.B. Shetty Memorial Institute of Dental Sciences (ABSMIDS)
3. K S Hegde Medical Academy (KSHEMA)
4. Nitte Usha Institute of Nursing Sciences (NUINS)
5. Nitte Gulabi Shetty Memorial Institute of Pharmaceutical Sciences(NGSMIPS)
6. Nitte Institute of Physiotherapy (NIPT)
7. Justice K S Hegde Charitable Hospital (JKSHCH)
8. NITTE (Deemed to be University) Centre for Science Education and Research (NUCSER)
9. Nitte Institute of Architecture. (NIA)
10. Nitte Institute of Communication (NICO)

B. Stake holders on campus or off campus includes

Students: UG, PG, Research
Employees (Permanent/ Temporary/ Contractual)
Faculty
Administrative Staff (Non-Technical / Technical)
Higher Officers
Guests

C. Resources Include

Network Devices wired/wireless
Wi-Fi Network
Internet Access
Official Websites, web applications
Official Email services
Data Storage
Mobile/ desktop / server computing facility
Multimedia Contents
Documentation facility (Printers/Scanners)

Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, senior officers, administrative staff (both teaching and non-teaching) and other employees
- Network administrators

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organisation, departments and individuals who are part of NitteDU community to understand how NitteDU policy applies to some of the significant areas and to bring conformance with stated policies.

Broadly Speaking the IT Policy of NitteDU stands not only for IT asset security and safety but also for the responsible use of IT facilities by the users of Nitte group of education.

It is to be noted that IT Policy of NitteDU is formulated and executed in consonance with service rules of NitteDU.

The Board of Management of the NitteDU will have the power to interpret the IT policy of NitteDU and the same shall be implemented by Vice chancellor of NitteDU. Systems Administrator shall receive the complaints regarding IT issues and the Registrar - NitteDU shall be the competent authority to take necessary actions regarding complaints and disciplinary actions in case of any misconducts. The said disciplinary action shall be initiated/taken by Registrar after approval from the Board of Management. Heads of the Institute/ Units/ Departments upon the report from point of contact shall have the power to give complaints to Registrar through Assistant Director- HR or Systems Administrator of NitteDU Regarding IT Issues/ problems.

However initially, as the IT literature among the employees of establishment is complex due to dynamic nature of information technology and varied superior subordinate relationship, Systems Administrator takes the responsibility of policy execution in step by step mode at each level, after obtaining due approval from the competent authority.

Policy Supporting Documentation	**Policy Support Contact**
Service and Conduct Rules NITTE (Deemed to be University)	Systems Administrator NITTE (Deemed to be University)

SECTIONS OF POLICY DOCUMENT:

1. Hardware Installation
2. Software Installation and Licensing
3. Web Site Hosting
4. Acceptable Use, Internet/Network (Intranet and Internet) Use
5. Acceptable Use, Email /E-mail Account Use
6. NitteDU Database Use and Information Dissemination
7. Access Controls, Use Accounts
8. Data Privacy
9. Protection against Computer virus and malware
10. Cybersecurity
11. Data Backup, Storage and recovery
12. General Information Security Management
13. Responsibilities of IT Department
14. Responsibilities of the Administrative Units
15. Guidelines on Computer Naming Conventions
16. Guidelines for hosting Web pages on the Internet/Intranet
17. Guidelines for Desktop Users
18. Green Computing
19. Video Surveillance

1. HARDWARE INSTALLATION

Network user community of NitteDU 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.

1.1. Who is primary user

An individual in whose room or section 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/ head of the institute should make an arrangement and make a person responsible for compliance.

1.2. What are end user computer systems

Apart from the client PCs used by the users**,** the NitteDU will consider servers not directly administered by IT department, 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 IT department, are still considered under this policy as "end-users" computers.

1.3. Power connection to computers and peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

1.4. 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.

1.5. 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.

1.6. Shifting computer from one location to another

Computer system may be moved from one location to another with prior written intimation to the IT Department as IT department maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room number. As and when any deviation (from the list maintained by IT Department) 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 IT department in writing/by email, connection will be restored.

1.7 Replacement of equipment

In general, ICT equipment should not be replaced until it fails, is uneconomical to repair or becomes unusable. The latter would generally occur when the equipment can no longer run the software or operating system at all, or at a reasonable, productive speed.

Although the standard manufacturer warranty for computer hardware is three or five years in

General. For laptops, users are advised to buy extended manufacturer warranties.

As desktop equipment is part of the ICT infrastructure used to deliver a range of core services, ICTS may, from time to time, issue notices that certain equipment should or must be replaced. This may occur prior to the recommended replacement periods below.

a. Desktop Computers

   Desktop computers may not be replaced before the end of a 7 year cycle.

b. LCD Monitors

   The expectation is that LCD monitors will last at least 8 to 10 years. Replacement is to

   be based on failure and is not bound to a particular cycle.

c. Second machines, tablets and laptops

   A staff member who has a laptop or desktop may be provided with a tablet where good cause is shown; however, where a staff member has a thin/light laptop there may be no justification for a tablet.Laptops may not be replaced before the end of a 7 year cycle.

d. Computer accessories

   Computer accessories such as keyboards, mice, stands and related accessories should be replaced on failure and are not bound to a particular cycle.

e. Printers

   Staff members must print to department/central printers whenever possible due the lower cost per page. Desk-based printers may be deployed only where a clear need exists and the purchase of ink jet printers should be avoided due to their higher operating costs.

f. Disposal of replaced hardware

   If ICT equipment cannot be re-deployed internally, then the processes as recommended by the Disposal of IT equipment policy must be followed. It is important that the disposal satisfies audit requirements, and is undertaken in the most economically advantageous manner.

1.8 Provision for standby equipment

When a Desktop computer, laptop or printer breaks down, on request of the concerned department's Head, the IT department will provide the standby desktop available at their disposal. The request should come in the official email to the IT department. The issue and receipt of the equipment will be made through official email communication. Inventory information is updated at both the departments. The IT department will install required licensed software with help of the concerned department.

The concerned department which received the standby ICT equipment will inform and return the device, when its equipment gets repaired. The IT department will coordinate with the designated vendors to repair the device and will certify the repair charges after obtaining the user feedback. It also makes sure that Vendor has taken sufficient care of the privacy of the data and equipment itself while repairing.

1.9 Power back-up for hardware installations

The continued and uninterrupted operation of the Nitte (Deemed to be university)'s Information and Communications Technology (ICT) equipment, servers at Data centre and network equipment is essential to the mission of the university. Towards this end, the university will maintain a two tiered power back-up - (1) diesel generators and a 20-kilowatt uninterruptible power system (UPS). The

purpose of this policy is to set forth guidelines for the operation, testing, and maintenance of these systems.

The Backup Power systems are designed to operate without significant manual intervention. They will start automatically when an interruption of electrical power from the utility power grid is detected and will continually operate until the power is restored. Normally, the only operational tasks required are to monitor the level of diesel fuel in the tank and to observe the scheduled automatic tests of the systems. The protected network and server equipment in the Data Centre draws its power from the UPS at all times, even when commercial power is available. The batteries are continuously recharged from this commercial power. When an interruption of electrical power from the commercial power grid is detected, the equipment which is connected to the UPS will continue to operate from the UPS with no interruption in service, But the generator will automatically start up to provide power to recharge the batteries. When the commercial power is restored and has become stable, the electrical service switches back to the commercial power grid and the generator shuts down automatically. The equipment protected by the Backup Power System UPS includes all servers in the Data Centre, essential network equipment, the telephone switchboard, the Help Desk, and the building access and alarm system.

In addition, Faculty/student used computers will be provided with small UPS which provide power during power supply changeover between grid and generator.

Testing at a predetermined time and day in each week, the generator will automatically start and will run for an interval long enough to warm up the oil.

Maintenance

The systems are initially under full warranty. Upon the expiration of those warranties, a maintenance agreement will be negotiated with the appropriate electrical contractors. UPS batteries are replaced at regular intervals.

1.10 General user responsibilities

ICT equipment located in common or open areas, and in computer labs must be secured with an approved security solution, such as a cable and lock. When unoccupied, rooms should be locked and alarmed. Similarly, staff should appropriately secure their equipment and offices.

Most pieces of ICT equipment contain sensitive electronic components that can be adversely affected by shock, heat, dust and liquid. Equipment should be located off the floor, preferably on a sturdy surface, away from direct sunlight and other heat sources, and situated such that other objects (i.e. books, papers, furniture) do not block the cooling vents.

Food and drink should always be kept away from any computer equipment. Most equipment can be safely dusted off with compressed (canned) air and wiped with a soft cloth slightly dampened with water only. Equipment should be turned off prior to cleaning or moving.

1.11. Non compliance

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

1.12. IT department interface

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

2. SOFTWARE INSTALLATION AND LICENSING POLICY

2.1. Anti-Piracy measures

Any computer purchases made by the individual departments/projects should make sure that such computer systems are installed only with licensed software (operating system, antivirus software and necessary application software).

Respecting the anti-piracy laws of the country, IT policy of NitteDU does not allow any pirated/unauthorized software installation on the NitteDU owned computers and the computers connected to the NitteDU campus network. In case of any such instances, NitteDU will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

2.2. Operating system and its updating

2.2.1.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.

2.2.2. NitteDU as a policy encourages user community to go for open source software such as Linux, Open office, Libre Office to be used on their systems wherever possible.

2.2.3. 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 user's responsibility to make sure that the updates are being done properly.

2.3. Antivirus software and its updating

2.3.1. Computer systems used in the NitteDU 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.

2.3.2. 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 user's technical skills, the user is responsible for seeking assistance from IT department.

2.4. 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 floppy, or CD or other storage devices such as pen drives as approved by IT department of NitteDU.

2.5 Service arrangements

In order to meet the needs of the University stake holders, some services will need to be outsourced to third parties. In such cases, the University mandates a Service Level Agreement (SLA) for all software and hardware related services in addition to issue of work orders with detailed terms and conditions. Service Level Agreements will list out expectations and quality of the service. It also provides remedies if service requirements are not met.

The SLA should include not only a description of the services to be provided and their expected service levels and quality, but also metrics by which the services are measured, the duties and responsibilities of each party, the remedies or penalties for breach, and a protocol for adding and removing metrics.

Faculty or university institution may take the help from the Legal department and Purchase department while formulating the draft and finalising the same considering all the factors related to Technology, Privacy protection, Finance and Legal issues. The service level agreement should comply with the rule of the land.

2.6. Non compliance

NitteDU 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 other users, confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, Departments, or even whole NitteDU. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

2.7. IT department interface

Systems Administrator 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 reg@nitte.edu.in if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The Systems Administrator will provide guidance as needed for the individual to gain compliance.

3. WEB SITE HOSTING

3.1. Official pages

Sections, departments, and associations of teachers/employees/students may have pages on intranet channel of the official web page of NitteDU. Official web pages must conform to the NitteDU web site creation guidelines for web site hosting. As on date, the NitteDU's IT department is responsible for maintaining the official web site of the NitteDU, viz., http: www.nitte.edu.in.

If department wants to have a page related to their department activity they may request IT department.

3.2. Web pages for E-learning:

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 NitteDU'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 NitteDU or other web sites. If a student publishes a fictional web site or a web site modelled 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:

A) **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 E learning purpose.

B) **Maintenance:**

If the pages are published on the E- learning 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.

C) **Content disclaimer:**

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

D) **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.

E) **Pages generated by class groups:**

Pages produced by class groups, if placed on the E-learning information server, will be placed on the server under the name of the designated group leader.

F) **Official pages:**

If web pages developed for E-Learning become the part of the "official" NitteDU page, they must be removed from the E-learning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

4. INTERNET/NETWORK (INTRANET AND INTERNET) USE

4.1. Overview and Purpose

The internet provides a source of information that can benefit every professional discipline represented in the NitteDU. This policy document delineates acceptable use of internet capabilities by NitteDU employees, volunteers, and contractors by means of equipment, facilities, internet addresses, or domain names owned, leased, or registered to NitteDU.

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

4.2. Coverage

Anyone who uses NitteDU equipment and facilities, and performed using internet protocol addresses and domain names registered to NitteDU. This includes, but is not limited to:

- Full and part time employees
- Volunteers authorized to use NitteDU resources to access the internet
- Departmental contractors authorized to use NitteDU equipment or facilities

All content that resides on or passes through NitteDU Information Resources, including computers, networks, and software, must conform to the NitteDU acceptable use Internet policy. This policy applies to internet access only. It does not cover the requirements, standards, and procedures for the development and implementation of NitteDU's information sites on the internet.

4.3.Roles and Responsibilities

A. Supervisors

Supervisors of employees, volunteers, and contractors have the final authority in determining whether an employee requires internet access to fulfil job requirements. Supervisors are responsible for:

i. Acquiring internet access for subordinate employees, as needed.

ii. Educating subordinate employees on restrictions against personal use of NitteDU networks, systems, and other electronic resources.

iii. Determination of appropriateness of subordinate employees' use of the internet. This includes judgement of the acceptability of internet sites visited and the determination of personal time versus official work hours.

B. System users

Use of computer equipment and networks to fulfil job responsibilities always has priority over personal use of equipment and networks. In order to avoid capacity problems and to reduce the susceptibility of NitteDU information technology resources to computer viruses and other malware, all internet users must:

i. Follow all security policies and procedures covering use of internet services.

ii. Refrain from any practice that might expose, compromise, or otherwise jeopardize organizational networks, computer systems, data files, and other electronic resources.

iii. Understand legal requirements and limitations regarding access, protection, and use of data covered by the “National Privacy Act”, copyright law, trademark law, and internal policy.

4.4. IP address allocation:

Any computer (PC/Server) that will be connected to the NitteDU network, should have an IP address assigned by IT department. 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 unauthorised from any other location. As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the IT department.

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.

4.5. DHCP and proxy configuration by individual departments /sections/ users:

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the NitteDU.

Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by IT Department. 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 user. Also it may be reported to HR department for disciplinary action.

4.6. Running network services on the servers:

Individual departments/individuals connecting to the NitteDU network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the IT department in writing and after meeting the requirements of the NitteDU IT policy for running such services. Non-compliance with this policy is a direct violation of the NitteDU IT policy, and will result in termination of their connection to the network.

IT department takes no responsibility for the content of machines connected to the network, regardless of those machines being NitteDU or personal property. IT department 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 NitteDU’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 NitteDU Network connects. NitteDU 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 IT department. 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 and disciplinary action.

4.7. Broadband connections:

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

4.8. Wireless local area networks:

A. This policy applies, in its entirety, to department or units wireless local area networks. In addition to the requirements of this policy, departments or units must register each wireless access point with IT department including point of contact information.

B. Departments/ units must inform IT department for the use of radio spectrum, prior to implementation of wireless local area networks.

C. Departments/ units 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.

4.9. Internet Bandwidth obtained by other departments:

Internet bandwidth acquired by any section, department of the NitteDU under any research programme/project should ideally be pooled with the NitteDU's internet bandwidth, and be treated as NitteDU's common resource.

Under particular circumstances, which prevent any such pooling with the NitteDU's internet bandwidth, such network should be totally separated from the NitteDU's campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the NitteDU's gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the NitteDU's 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 IT department.

4.10. Policy

A. Internet Access

If an employee's supervisor determines that Internet access is in the best interest of NitteDU, the employee may, within the limits set forth below, use NitteDU networks and equipment to access the internet. Employees who do not require access to the Internet as part of their official duties, may not access the internet using NitteDU's facilities under any circumstances.

B. Permitted Use

i. Access to online job related information, as needed, to meet the job requirements.

ii. Participation in newsgroups, chat sessions, email communications, and online discussion groups, provided those communications activities have direct relationship to the user's job responsibilities.

iii. Access to online content to develop or enhance job related skills. It is expected that these skills will be used to improve the accomplishment of job related work assignments.

C. Use of internet and company networks for non-business purposes

NitteDU's computer systems are for official and educational use; however, when certain criteria are met, departmental users may use information resources for personal activities. All personal internet use through business information resources are subject to the following restrictions:

i. They must not degrade or otherwise impede normal job performance

ii. They do not incur direct costs to NitteDU

Since employees who use NitteDU's information resources may be perceived by others to represent NitteDU, employees may not use the internet for any purpose that could reflect negatively on NitteDU or its employees. Personal opinions expressed over the course of online communications activities should include a disclaimer stating that they do not reflect official positions of NitteDU.

Employees may not initiate non work related internet sessions using NitteDU information resources from remote locations. For example, employees shall not log into organizational resources from home or other remote locations to engage in non-job related activities. Personal use of NitteDU's Information Resources to access the Internet is restricted to approved users; it does not extend to family members or other acquaintances.

D. Reasonable security and privacy precautions

i. All files downloaded from the internet must be scanned for viruses using approved software and current virus detection software.

ii. Any corporate data posted on internal web sites must not be available to access by a broader online audience than is appropriate for the materials themselves.

iii. All sensitive business materials transmitted over external networks must be encrypted.

iv. No files or documents may be sent or received that may cause legal liability for, or embarrassment to the NitteDU.

E. Use of internet client and browser software

i. All software used to access the internet must be part of the NitteDU standard software suite or approved by IT management.

ii. IT staff must update Internet clients and browsers as vendor provided security patches are released.

iii. Internet clients and browsers must be configured to use the NitteDU firewall http proxy.

F. Prohibited use

Employees may not use NitteDU's information resources, either during working hours or on personal time, to:

i. Access, retrieve, or print text and graphics information that violate the acceptable use policy

ii. Engage in unlawful activities or other activities that could in any way discredit NitteDU

iii. Engage in personal commercial activities, including offering services or merchandise for sale, non-business related online purchasing, and personal commercial advertising. Where online commercial transactions are permitted as part of legitimate job functions, transactions are subject to NitteDU's procurement rules.

iv. Engage in any activity that would compromise the security of NitteDU's systems, resources, or networks

v. Engage in any fund raising activity, endorse any product or services, participate in any lobbying activity, or engage in any active political activity

vi. Access or download video and voice from the internet, except in the service as an approved job function.

vii. Store personal files obtained via the Internet on NitteDU's drives, servers, or other devices

G. Enforcement

i. All activity on NitteDU's information resources is subject to monitoring by management, H.R personnel, system and security personnel, legal personnel, and other authorized staff. Monitoring includes logging and review. Use of NitteDU's systems constitutes consent to monitoring.

ii. All files and documents—including personal files and documents—stored on or transmitted by company information resources are subject to managerial review and may be accessed in accordance with this policy.

iii. Violation of this policy may result in disciplinary action, including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of NitteDU's information resources access privileges, civil, and criminal prosecution.

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

5. EMAIL/EMAIL ACCOUNT USE

5.1. Overview and Purpose

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the NitteDU's administrators, it is recommended to utilize the NitteDU's e-mail services, for NitteDU's formal communication and for academic and 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 NitteDU communications are official notices from the NitteDU to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general NitteDU 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://nitte.edu.in**with their **UserID** and **password**. For obtaining the NitteDU's email account, user may contact IT department for email account and default password by submitting an application in a prescribed proforma through head of the institute/units.

The NitteDU's electronic mail (email) facility offers employees and contractors an efficient way to communicate with others inside, and outside (via Internet) the NitteDU using the organization's computer systems. The purpose of this policy is to:

● Establish rules for the creation and transfer of information through the NitteDU's internal email system.

● Prevent unintended disruption or degradation of network communications and the efficient operations of email systems.

5.2. Coverage

All individuals authorized to use any NitteDU's information resource with the capacity to send, receive, or store electronic mail.

5.3. Policy

A. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

i. The facility should be Used primarily for academic and official purposes and to a limited extent for personal purposes. i.e. NitteDU employees may make incidental personal use of email but any incidental email usage for personal use may not interfere with official duties, must have a minimal effect on the organization, and must be consistent with official duties, must have minimal effect on the organization, and must be consistent with standards of ethical conduct.

ii. Using the facility for illegal/ commercial purposes is a direct violation of the NitteDU'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.

iii. Authorised NitteDU email users are not permitted to forward NitteDU email or attachments to personal accounts managed by public email or internet access service providers where the information might be compromised.

iv. NitteDU employees and contractors are not authorized to use the email system to send sensitive information via the internet where information might be intercepted.

v. System Users must must not send, forward, receive or store confidential or sensitive NitteDU information utilizing non NitteDU accredited mobile devices. Examples of mobile devices include, but are not limited to, personal data assistants (PDAs), two way pagers, tablets and cellular telephones.

vi. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

vii. User should not open any mail or attachment that is from suspicious/ unknown source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or look 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.

viii. 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.

ix. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

x. While Using the computers that are shared by other user 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.

xi. Impersonating email account of others will be taken as a serious offence under the NitteDU's IT security policy.

xii. It is ultimately each individual's responsibility to keep their e-mail account free from violations of NitteDU's email usage policy.

xiii. All the mails detected as Spam mails go into SPAM MAIL folder of the respective user's 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.

xiv. The above laid down policies particularly 1 to 12 are broadly applicable even to all the email services that are provided by other sources, as long as they are being used from the NitteDU's campus network, or by using the resources provided by the NitteDU to the individual for official use even from outside.

B. Appropriate use of email

Appropriate use of the NitteDU email system includes generating and sending emails regarding:

i. NitteDU's mission and program related activities

ii. Other related and endorsed activities with respect to NitteDU

iii. Subject to the limitations contained in this email policy statement, brief occasional personal messages

C. Inappropriate use of email

NitteDU email facility may not be used to:

i. Send email intended to intimidate or harass individuals or organizations

ii. Conduct personal business

iii. Send unsolicited messages to large groups, except as required to conduct organizational business

iv. Sending excessively large messages or messages with attachments larger than 20mb

v. Send or forward email that is likely to contain computer viruses

vi. Sending or forward personal messages to everyone in the company directory or other large user groups

vii. Send or forward chain letters

viii. Conduct political lobbying or campaigning

ix. Violate copyright laws by inappropriately distributing protected works

D. Email system users may not:

i. Represent themselves as anyone other than themselves when sending email, except when explicitly authorize to do so in an administrative support role.

ii. Use unauthorized email software

iii. All sensitive NitteDU material transmitted over external network must be encrypted.

iv. Email system users must not give the impression that the user is representing or making statements on behalf of NitteDU, except under condition of explicit authorization.

v. The following disclaimer must be included in all messages sent through the email system: “The opinions expressed in this message are my own, and not necessarily those of my employer."

vi. For other terms and criteria of system use, refer to the organization’s policy on acceptable use: internet.

E. Enforcement

i. All activity on NitteDU’s information resources is subject to logging and review

ii. If an inappropriate email is brought to our attention, the sender may be directed by either the email postmaster or the computer security officer to retract the message. Inappropriate or unauthorized email may be retracted by the postmaster if the sender is not available.

iii. Violation of this policy may result in disciplinary action, including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of NitteDU’s information resources access privileges, civil and criminal prosecution.

6. DATABASE USE AND INFORMATION DISSEMINATION POLICY

6.1. Introduction:

This Policy relates to the databases maintained by the NitteDU administration under the NitteDU's E-Governance. Data is a vital and important NitteDU resource for providing useful information. Its use must be protected even when the data may not be confidential. NitteDU 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 NitteDU's approach to both the access and use of this NitteDU's resource.

6.2. Policy:

A) Database Ownership: NitteDU is the data owner of all the NitteDU's institutional data generated in the NitteDU.

B) Custodians of Data: Individual sections or departments generate portions of data that constitute NitteDU's database. They shall have 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 E Governance, Management Information System requirements of the NitteDU may broadly be divided into seven categories. These are:

i. HUMAN RESOURCE INFORMATION SYSTEM (HRIS)

ii. STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)

iii. FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)

iv. ASSET TRACKING/PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (ATMS)

v. LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)

vi. DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

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

i. The NitteDU's data policies do not allow the distribution of data that is identifiable to a person outside the NitteDU.

ii. Data from the NitteDU's data base including data collected by department or individual faculty and staff is for internal NitteDU purposes only.

iii. One's role and function define the resources that will be needed to carry out one's official responsibilities/ rights. Through its data access policies, the NitteDU makes information and data available based on those responsibilities/ rights.

iv. Data directly identifying a person and his/ 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 Registrar- NitteDU.

v. Requests for information from any courts attorneys etc are handled by the Registrar's office of the NitteDU and departments should never respond to requests, even with a writ/court order. All requests from law enforcement agencies are to be forwarded to the office of Registrar - NitteDU respectively for response.

vi. 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 NitteDU or its departments.

vii. All reports for UGC, MHRD and other government agencies will be prepared/ compiled and submitted by the Registrar, Controller of Examinations and Finance Officer of the NitteDU.

viii. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

ix. Tampering of the data base by the department or individual user comes under violation of IT Policy.

x. Tampering includes but not limited to:

(a) Modifying/deleting the data items or software components by using illegal access methods.

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

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

(d) Trying to break security of the database servers.

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

6.3. Information Dissemination Policy

A) It should always be kept in mind that the apex custodian for information, data, data base and emails of NitteDU shall be “The Registrar- NitteDU”. However either it be “internet or intranet', “email or data base”... there will be many informations or data which may be disseminated and at the same time there are many information or data on which strict confidentiality may have to be maintained. Respective heads of institute, unit, hospital, department, unit, section... under which such informations, emails, data, data base... are maintained shall beits sub custodians.

B) Wheneverany information, data, data base or email of NitteDU is requested or sought by any external person or body (whether it be public/ statutory bodies or private bodies /persons) such instances should be immediately submitted and brought to the notice of respective custodian (The Registrar-NitteDU) for further actions on that and further actions on the same shall be carried out either under their approval or authorization.

C) The information or data sought under/through courtorders, summons, notices, shallbe strictly and immediately submitted and brought to the notice of “The Registrar- NitteDU” for further actions.

7. ACCESS CONTROLS AND USER ACCOUNTs

7.1. Overview and Purpose

NitteDU must balance employees needs to access systems and information with the organizational obligation to control access for the purposes protecting information confidentiality, integrity, and availability. Account passwords are a mainstay of information security controls. This policy establishes management controls for granting, changing, and terminating access to automated information systems, controls that are essential to the security of NitteDU's information systems.

7.2. Coverage

All full and part time employees, contractors, and other personnel who use NitteDU's Information Resources.

7.3. Roles and Responsibilities

A. Systems Administrator

i. Oversees password administration for NitteDU

ii. Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords

iii. Acts as an Information Security Officer (ISO)

iv. Reviews and validates access and rights records at least once per 3 months to confirm continuing need for access

v. Prepares policy guidelines for the creation, safeguarding, and control of passwords

vi. Approves access rights and passwords for privileged accounts for NitteDU

vii. Issues passwords for privileged accounts.

viii. Issue and manage passwords and account rights for systems and applications under their control

B. Supervisor/ Point of Contact

i. Communicates system access and password requirements to the user community

ii. Informs the Information Security Officer (ISO) if any access or system rights should be changed or removed

iii. Immediately informs the IT Department if a password is known or suspected to be compromised

C. System users

i. Protect password confidentiality

ii. Immediately notify supervisor if a password is known or suspected to be compromised

7.4. Policy

A. Password rights administration

i. Access to NitteDU's Information resources must be controlled.

ii. Access to NitteDU's information resources must be based on an approved system access request form for each discrete system.

iii. Access rights are granted based on the principle of "least privilege": Access is granted only to systems and application necessary for the performance of official duties.

iv. Supervisor /Point of Contact and Systems Administrator(ISO) must approve employee access rights to NitteDU information Resources.

v. The Registrar-NitteDU must approve Supervisor and Systems Administrator to access rights to NitteDU's Information Resources.

vi. Privileged access passwords (such as those belonging to Systems Administrators) must be changed at least once in every 2 months or when necessary due to employment termination, actual or suspected password compromise.

vii. Information Security Officers and Systems Administrators shall not allow generic or group access credentials, including passwords.

viii. Contractor accounts and access privileges must be terminated on the contract expiration date. Contractor supervisors are required to inform System Administrators of new and changed contract effective dates that are likely to affect account access permissions.

ix. Vendor or service accounts included in acquired software or used for software development must be deleted prior to software deployment.

x. Any default passwords must be changed on all systems prior to connection to any network, even in pre deployment testing.

xi. Administrative account passwords must be changed promptly upon departure of personnel or suspected compromise.

xii. User accounts must be disabled promptly upon departure of personnel. If a user knows or suspects that the confidentiality of their password has been compromised, they must immediately change the password.

B. Password requirement

i. Passwords (login) are required on all NitteDU's information systems

ii. Each individual users are assigned unique login credentials comprising, at minimum, at unique user name and password

iii. Passwords must conform to the following criteria:

iv. At least eight characters in length

v. Consist of a mix of alpha, numeric, and special characters

vi. Exclude dictionary words

vii. Exclude portions of associated account names (e.g., user ID, login name)

viii. Exclude common sequential character strings (e.g., "abc" or "1234")

ix. Exclude simple keyboard patterns (e.g., "asdf")

C. Automated controls

i. To reduce the risk that an unauthorized party can gain system access by guessing a user's password, the NitteDU system(s) shall limit invalid login attempts to three. After three unsuccessful login attempts, the NitteDU system(s) must automatically "lock out" the attempting user for not less than 1 hour. **Note:** For critical systems, the policy administrator may wish to specify that "locked out" users must contact a Systems Administrator in order to reactivate a "locked" account.

D. Password protection

i. Users must change passwords immediately after the initial login to any NitteDU system(s) Information Resource.

ii. Users must not disclose or otherwise allow third party use of their unique account credentials (User IDs and Passwords).

iii. Passwords must be changed at least once in every 2 months.

iv. Passwords may not be reused for at least 5 consecutive login change cycles

v. Passwords must not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, or terminal hot keys.

vi. Passwords must be not rendered in readable form through publicly visible media by any application, printer, web server, or other mechanism.

vii. Passwords must not be stored in readable form in any application, file, or database.

E. Enforcement

Gross negligence or willful disclosure leading to illicit exposure of NitteDU's information may result in prosecution for misdemeanour or felony resulting in fines, imprisonment, civil liability, and/or dismissal.

8. DATA PRIVACY

This policy section governs users' relationship with NITTE (Deemed to be University) regarding the use of the website and its hosted web applications. The university website provides general information regarding the institutions/units and its services. Information available in this website should not be assumed to be complete or up-to-date. The web applications are designed for the university's particular administration.

With regard to third party developed softwares/application which deals with student/faculty personal information, University executes a Non Disclosure agreement (NDA) in the first phase, that is procurement itself. Without NDA, university institutions are not allowed to transfer/provide student/faculty information to any third party.

8.1. Privacy Statement

NITTE (Deemed to be University) website is operated by the IT department of NITTE (Deemed to be University). Visitors to www.nitte.edu.in are guaranteed privacy. Information collected on https://nitte.edu.in is kept private and never shared with other organizations.

8.2. Measuring Audiences

User IP (Internet Protocol) address is used to gather broad demographic information. NITTE logs IP addresses and browser types for systems administration purposes. These logs are analyzed constantly to improve the value of the materials available on this website. IP address also helps us diagnose problems with the university's server and administer the website. IP addresses do not provide us with any identifiable personal information. This means users' sessions will be tracked, but will remain anonymous to us in case of the website which does not require login to view the information.

8.3. Cookies

In order to better understand the way our websites are used by visitors, NITTE employs the use of cookies, a small file that stores information on users' hard disk drives. NITTE uses information derived from cookies strictly for tracking usage and developing site improvements.

8.4. Outside Links

This site contains links to sites outside www.nitte.edu.in and other sites may provide links to this site. NITTE is not responsible for the privacy practices, or the content, of such other websites. These links are provided for user convenience only. NITTE does not control these other sites and assumes no liability or responsibility for them, including any content or services provided to users by such sites. Users should not consider any link to or from another site as an endorsement of that site by NITTE, unless NITTE expressly states so.

8.5. Personal Information

Users agree that NITTE may share certain information about the user. Users agree that, should the user elect to supply it, NITTE may use user name, email address, physical address, telephone or other data to communicate with the user either by itself or through any of its designates. Users may request to have this information modified or deleted from our records. NITTE may use this information as necessary to enforce these "Terms". NITTE will not sell this information to any other party.

These "Terms" are severable to the extent any term is deemed invalid, illegal or unenforceable. NITTE's failure to enforce any provision of these "Terms" shall not be deemed a waiver of that or any other provision of these "Terms".

Users' use and continued use of the NITTE's Site reflects user agreement to these "Terms" and any modifications of these "Terms" made by NITTE.

8.6. Submitting Personal Information

Users can submit information to www.nitte.edu.in in several places on the website. A 'Contact Us' form allows customers to request information. The form requests visitors contact information such as their email address and/or mailing address. Contact information from the feedback form is used to send responses or information requested by our users. This information is never shared; it is used only for our replies.

8.7. Site Security

This site has security measures in place to protect the loss, misuse and alteration of the information under our control.

A. Permission

1. NITTE gives the user limited personal permission to use the website. User permission to use the web site is limited in a number of ways. For example, users may only download or print material contained on this Site for non-profit purposes. Any commercial use, such as selling content, creating course packs, or posting information on another website is prohibited.

2. User may not:

- Frame all or part of the website.
- Change or delete any proprietary notices from materials downloaded or printed out from the website.
- Systemically download or print materials from the website.
- Transmit or provide any data from the website to a third party.
- Use the website in a manner contrary to any applicable law. User permission terminates immediately, without any further action by NITTE, if the user breaches these "Terms".

3. Users may not transfer or assign user permission to any other party.

4. NITTE is the owner or licensee of all rights in the website, its content, software, and services. Users have no right to such content, software or services if not expressly granted in this agreement.

5. "NITTE" and the logos or other proprietary marks of NITTE's licensors and partners are trademarks of NITTE or its licensors and partners. No right, title or interest in those trademarks is granted to users in this agreement.

6. The site is provided "As Is ".

7. Services provided through and information contained on the site are provided as is and as available. NITTE makes no, and hereby disclaims any, warranty of any kind, express or implied, including but not limited to the implied warranties of title, non-infringement, merchantability and fitness for a particular use or purpose. Further, NITTE disclaims any warranty that the site will be available at all times or will operate without interruption or error. NITTE makes no warranty as to the reliability, accuracy, timeliness, usefulness, adequacy, completeness or suitability of the services or information provided through the site.

8. Users alone are responsible for use of the site.

9. Users agree to be solely responsible for use of this website.

10. NITTE, its officers, directors, employees, agents, and information providers shall not be liable for any damages users may suffer or cause through use of the site, even if advised of the possibility of such damages.

11. NITTE, its officers, directors, employees, agents, and information providers shall not be liable for any direct, indirect, incidental, special, consequential, or punitive damages arising out of use of or inability to use the site.

12. These limitations shall apply whether the asserted liability or damages are based on contract (including, but not limited to, breach of warranty), tort (including, but not limited to, negligence) or any other legal or equitable grounds.

13. Users agree to indemnify and hold NITTE harmless for any claims, losses or damages, including attorney's fees, resulting from the user's breach of these terms or use of this website.

B. Children's Guidelines

Nitte does not knowingly collect identifiable personal information from children under age.

A parent or guardian must initiate any requests for information from children under the age of 13 on their behalf. We encourage parents to supervise children when they browse the Internet.

Privacy Protection NITTE does not utilize direct mail services for "telemarketing by third party" so that user information will not be used for solicitation by third parties.

9. PROTECTION AGAINST COMPUTER VIRUS AND MALWARE

9.1. Overview and Purpose

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. The purpose of the Computer Virus Detection Policy is to describe the requirements for dealing with computer virus, worm and trojan horse prevention, detection and clean-up.

9.2. Coverage

The NitteDU Computer Virus Detection Policy applies equally to all individuals that use any NitteDU's information resources.

9.3.General Terminology

A. Email

A message, image, form, attachment, data, or other communication sent, received, or stored by an electronic mail system.

B. Incident

A recognized attempt by an unauthorized party to access a trusted network, or an attack on an information system. The term encompasses unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; loss of accountability or damage to any part of the system; or changes to information system hardware, firmware, or software characteristics with or without users' knowledge, instruction, or intent. Incidents are generally perceived as malicious attempts to violate or degrade the confidentiality, integrity, and/or availability of information resources.

C. Server

1. A computer program that provides services to other computer programs on the same or another computer

2. A computing machine that runs a server program

D. Trojan

A destructive program—usually a virus or worm—hidden in another piece of software, such as a game or graphics program. Trojans are typically distributed with malicious intent for the purpose of harvesting data, disrupting computing activities, or enabling unauthorized access to restricted networks or devices.

E. Virus

A program that is attached to or embedded in an executable file or vulnerable application. Viruses deliver payloads that can range from annoying to extremely destructive. There are many types of viruses. A file virus, for example, executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

F. Worm

A software program that, once downloaded to a computer system, copies of itself elsewhere on the system. Today the term is usually used to describe software that maliciously propagates itself over a network, often with the intent of overloading network capabilities. Worm is often used synonymously with "virus" however.

9.4. Policy

A) All workstations whether connected to the NitteDU’s network, or standalone, must use the NitteDU's approved virus protection software and configuration.

B) The virus protection software must not be disabled or bypassed.

C) The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

D) The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

E) Each file server attached to the NitteDU network must utilize NitteDU's approved virus protection software and set up to detect and clean viruses that may infect file shares.

F) Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the point of contact or supervisor or System's Administrator for further actions.

9.5. Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of NitteDU's information resources access privileges, civil, and criminal prosecution.

10. CYBER SECURITY

As the first step towards cyber security, university will allow and use only licensed software. Faculty and student are to be educated to use devices only with licensed software. Local area network and WiFi network will be protected by robust Firewall with Intrusion Detection and Prevention system to block harmful traffic from both ways; from internet and at the local intranet level.

All the computers must have a licensed Antivirus system which is regularly updated. Updation is to be verified by IT department's staff with regular intervals and recorded with user signature.

Users will be regularly educated through email about the Intellectual property rights. If any user downloads more than 6GB of data using the university LAN computer, verification is done through official communication to check whether data is downloaded for academic purposes.

Each LAN connected computer will be 'Administrator password' protected, which will not be known to the user. Faculty or students can login to the system using a User password which does not allow installation of any software. Periodic inspection will be carried out by IT - in - Charge at the campus units or institutions. In addition, a surprise inspection will be carried out by the Systems Administrator and a report will be submitted to the Registrar.

11.DATA BACKUP, STORAGE AND RECOVERY

11.1. Overview and Purpose

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors. The purpose of this Data Backup and Storage Policy is to establish the rules for the backup and storage of NitteDU's electronic information.

11.2. Coverage

This Data Backup and Storage Policy applies to all individuals within the NitteDU who are responsible for the installation and support of information resources, individuals charged with information resources security; and data owners.

11.3. Services

Information services may have existing contracts for offsite backup data storage. These services can be extended to all entities of NitteDU upon request.

11.4. Policy

1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
2. The NitteDU's Information Resources backup and recovery process for each system must be documented and periodically reviewed.
3. Any vendor(s) providing off site backup storage for NitteDU must be cleared to handle the highest level of information stored.
4. Physical access controls implemented at off site backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest sensitivity level of information stored.
5. A process must be implemented to verify the success of the NitteDU electronic information backup.
6. Backups must be periodically tested to ensure that they are recoverable.
7. Signature cards held by the offsite backup storage vendor(s) for access to NitteDU backup media must be reviewed annually or when an authorized individual leaves NitteDU.
8. Procedures between NitteDU and the offsite backup storage vendor(s) must be reviewed at least annually.
9. Backup media must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar coding system:
    a. System name
    b. Creation date
    c. Sensitivity classification [Based on applicable electronic record retention regulations]
    d. NitteDU's contact information
10. Guidelines for standalone systems

    A. Data backup Standards:

    1. Critical data, which is critical to the university, must be defined by the university in consultation with ICT and must be backed up. Backup data must be stored at a backup location/Cloud storage that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site).

2. Data backed up must at least be tested quarterly.

3. Procedures for backing up critical data and the testing of the procedures must be documented by the IT department. These procedures must include, as a minimum, for each type of data and system:

a. A definition of the specific data to be backed up;

b. The type(s) of backup to be used (e.g. full back up, incremental backup, etc.);

c. The frequency and time of data backup;

d. The number of generations of backed up data that are to be maintained (both onsite and offsite);

e. Responsibility for data backup;

f. The storage site(s) for the backups;

g. The storage media to be used;

h. Any requirements concerning the data backup archives;

i. Transport modes; and

j. Recovery procedure of backed up data.

B. Data Backup Selection and Procedures

a. All data and software essential to the continued operation of the university, as well as all data that must be maintained for legal purposes, must be backed up. All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.

b. Full back up and Incremental backup schedule should be fixed with consultation of the IT department.

c. The schedule of the backup should be defined by the IT department.

d. The IT Department should determine the quantity of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location.

e. Data backup may be done to cloud storage and to a local computer.

f. As a university has a hospital under its management, Data should be retained in line with current legislative requirements. Monthly backups must be saved for one year. Yearly backups must be retained for five consecutive financial years.

g. Recovery of Backup data: Documentation of the restoration process must include:

- Procedures for the recovery
- Provision for key management should the data be encrypted.

Recovery procedures must be tested at least quarterly and Disaster Recovery procedures must be tested at least yearly. Recovery tests must be documented.

11. Disaster Recovery

For most important and time-critical data, a mirror system, or at least a mirror disk may be needed for a quick recovery. The University will plan and establish such a system.

12. Enforcement: Violation of this policy may result in disciplinary action, including but not limited to performance penalties, employment termination, contract invalidation, civil action, and criminal prosecution. Additionally, violators may lose access privileges to NitteDU's information resources.

12. GENERAL INFORMATION ON SECURITY MANAGEMENT

12.1. Overview and Purpose

The NitteDU' s computer network or systems is a critical resource that connects people, business processes, systems, and information resources. Network security procedures help protect the network both from external, malicious threats and from internal errors that might compromise network connections and degrade the confidentiality, integrity, and/or accessibility of information resources connected by the network. This procedures document sets forth guidelines for the maintenance of network security. Compliance with these guidelines should conform to IT management policies

12.2. Coverage

All personnel who have access to the NitteDU information resources.

12.3. Roles and Responsibilities

A. Systems Administrator

- **i.** Ensures IT resources are adequately safeguarded
- **ii.** Develops and implementing an overall network security plan for the NitteDU systems.
- **iii.** Issues guidelines and procedures
- **iv.** Provides oversight for the NitteDU network security.
- **v.** Maintains current inventory of sensitive systems and a schedule for testing systems contingency plans.

12.4. Policies, Procedures, and Guidance

The IT department has overall responsibility for the security of the NitteDU's network. It is the responsibility of that department to ensure that all laws, rules, policy, procedures, and guidelines applicable to network security are implemented and enforced.

A. Delegation of authority

For every system, the IT department must designate a role or individual that is responsible for system security. This role, which will be referred to as the Point Of Contact (POC), may be an employee or contractor. In the latter case, security responsibilities must be specified in the terms of the contractor's engagement contract.

The Point of Contact must know the nature of the information processed by the system (or an application on the system) and be able to apply and manage appropriate security controls. The IT department must provide oversight and direction to the Point of Contact for network security purposes. These responsibilities should be delegated in writing by the concerned authority.

B. Security plans

Every system must have an IT Security Plan that documents the security posture at a particular point in time. The System Administrator or its appointee is responsible for network. System owners are responsible for systems or applications on the network.

The IT security plan reports the outcome of the IT security planning process. IT security plans are considered sensitive documents and must be protected as such, although they must also be available to the IT department and other security, application, and project and program managers, as needed to execute security plan

requirements. In addition, the IT security plan must be made available to officials such as database owners and authorized external and internal auditors, as required. The IT security plan must be updated whenever major changes to equipment, software, configurations, or network infrastructure affecting an application or system.

IT security plan content must be reviewed periodically, at least once in six months, to ensure it remains relevant and accurately reflects the Organization's risk posture, business processes, and technology environment. An IT security plan remains in effect until a new plan is issued; however, the maximum time that may elapse before issuing a new plan is one year.

D. Procurement (Acquisition)

The Systems Administrator must certify every significant planned IT procurement in order to ensure that the proposed resource meets information security requirements. This certification requirement is further described in the security life cycle standard.

E. Periodic Review

The Systems Administrator must periodically perform risk, threat, and/or vulnerability reviews of information security controls in order to ensure that security plans continually reflect technology changes and upgrades, risk profiles and organizational risk tolerance, policy and procedure updates, and shifting organizational roles. The scope and frequency of control reviews may vary, depending on the constancy of the operational environment and the degree of system or process risk that management deems acceptable. The maximum time that may elapse between risk, threat, and/or vulnerability analysis is six months.

F. Designated Approval Authority (DAA)

The Systems Administrator or a designated representative acts as a Designated Approval Authority. As such, he/she has overall responsibility and authority to accept or defer acceptance of information of security controls. The Systems Administrator may be responsible for issuing system security certification and accreditation statements that records the decision to accept security controls.

The DAA must be at an organizational level such that he/she has authority to

(a) evaluate the overall mission requirements of information systems and

(b) provide definitive directions to systems developers or owners relative to the risk in the security posture

of the systems.

By signing the authorization “to process,” the DAA accepts responsibility for the level of risk inherent in the system. Before a new, or significantly changed system or application can become operational, the following must occur:

- Assurance by Systems Administrator that an IT security plan is in place, upto date, and being followed
- Authorization by Systems Administrator in writing that the use of the system, based on the IT security plan, presents an acceptable level of risk to the system and the information it processes. Systems must be reauthorized periodically, every time they undergo a significant change, or at least once every six months. A record of the written authorization must be associated with the IT security plan.

G. Systems continuity/Contingency plans

A Systems continuity/Contingency plan is required for each general support system and major application. Plans must be approved in writing and retained by Systems Administrator. Systems continuity and contingency plans are considered sensitive documents and must be protected as such. In addition, they must be made available to officials such as database owners, internal auditors, and authorized external auditors, as required. Systems continuity/contingency plans must be updated periodically, at least once every six months. Plans must also be tested as needed, not less frequently than once every six months.

H. System Documentation Reviews

At least once every six months, System Administrators must review the documentation for systems that are under the control of their organization. The purpose of these reviews is to ensure that significant changes to systems are brought to management's attention and that any necessary corrective actions can be planned, budgeted, and implemented. If no significant changes have occurred, this status should be reported to the Systems Administrator, who shall notify the designated representative.

I. Security Awareness and Training:

The Systems Administrator is responsible for ensuring that all the NitteDU information system users understand network security goals, controls, and requirements. New employees should receive general information security training within six months of start of employment. All general users must receive periodic information security awareness training. Executives and managers must receive IT security awareness training at the program management level. System Administrators, database owners, and system security professionals must receive security awareness training associated with their system access and responsibilities.

J. Incident reporting and response

The Systems Administrator ensures that policies and procedures are established and maintained for recognizing, responding to, and reporting information security incidents. The Systems Administrator appoints in writing a formal Incident Response Team and provides direction to that team. The Systems Administrators reports incidents to the Registrar- NitteDU, as required in accordance with the NitteDU's guidelines. The Systems Administrator has ultimate responsibility for the safeguarding of corporate and information assets. In the event that the NitteDU's information resource *or system* is compromised, producing loss of system confidentiality, integrity, or availability, the Systems Administrator must discuss with the sub custodians of the affected system(s) whether to investigate the incident. If investigation is indicated, the Registrar ensures that proper forensic procedures are implemented to preserve evidence. The Registrar works closely with the ISO, System Administrator, and relevant business units throughout the investigative and prosecution process. If the NitteDU Web site or other public facing system is compromised, the Systems Administrator also works closely with the internal Public Relations team. All external inquiries are directed to the Public Relations team.

K. Enforcement

Gross negligence or wilful disregard of these procedures can result in disciplinary action that may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of the information resources access privileges, civil, and criminal prosecution.

13. RESPONSIBILITIES OF IT DEPARTMENT

13.1. Responsibilities with respect to network:

A. Campus Network Backbone Operations:

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

ii**.** IT department operates the campus network backbone such that service levels are maintained as required by the NitteDU's sections, 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 IT department.

ii. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of IT department. It essentially means exactly at which location the fibre optic based backbone terminates in the buildings will be decided by the IT department. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fibre optic, wireless or any other media) is also the responsibility of IT department.

iii. IT Department 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 NitteDU 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 NitteDU's internet links.

C. Network expansion

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

D. Wireless Local Area Networks:

i. Where access through Fibre Optic/UTP cables is not feasible, in such locations IT department considers providing network connection through wireless connectivity.

ii. IT department is authorized to consider the applications of sections, departments, or divisions for the use of radio spectrum from IT department prior to implementation of wireless local area networks.

iii. IT department 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. Global naming and IP addressing

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

G. Providing net access IDs and email accounts

IT department 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 NitteDU upon receiving the requests from the individuals on prescribed proforma.

H. Network operation centres

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

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

I. Network policy and technology standards implementation

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

J. Receiving complaints

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

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

The designated person in IT department receives complaints from the users and coordinates with the user and service engineers-hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service:

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

L. Disconnect Authorization

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

13.2. Responsibilities with respect to hard ware and peripherals

A. Maintenance of computer hardware and peripherals

IT department is responsible for maintenance of the NitteDU owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to them.

B. Technical support for University's computing hardware, accessories and services

i. IT department may receive complaints from users, if any of the particular computer systems are causing network related problems.

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

iii. The designated person in IT department receives complaints from the users of these computer systems and coordinates with the service engineer or technical team of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. Technical support for personally owned devices

NitteDU subsidizes purchase laptops / notebooks for it's teaching staff. The ownership of such devices rests with the teaching staff. For students, the University follows a Bring Your Own Device policy. In view of this, the IT Support Centre technical consultants will be available in person or by phone to assist with campus applications and services or to help staff/students with personally owned computers or devices. This procedure applies to Information Technology Services (ITS) staff who provide direct on-call support for those systems and those parts of the University's information technology (IT) infrastructure deemed critical. It applies to direct support and management of the systems and infrastructure, and to support for system owners. It does not apply to end-user support, with the exception of some end user support for a limited number of Executive staff.

Services to be made available:

1. Supporting and training web applications usage developed by or used at university
2. Troubleshooting problems on student, faculty, or staff computers
3. Installing operating systems and software. Software licenses must be provided by the customer.
4. Removing spyware and viruses
5. Removing unwanted software
6. Installing wired or wireless networking cards
7. Troubleshooting network problems
8. Taking reports of problems with the wired or wireless network
9. The centre will run diagnostics and perform basic fixes at no cost for members of the campus community. If IT staff determines that the system needs a computer repair service, will contact the authorised service provider.

Obligations of on-call staff

While on call, the staff member will keep their mobile telephone within network coverage and switched on, and be in a position to answer or respond to calls within 30 minutes and be able to attend the university campus if required or obtain remote access within one hour.

D. Installation of un-authorized software

IT department 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 any user come across any applications that are interfering with the network operations or with the IT policies of the NitteDU, such incidents should be brought to the notice of the IT department.

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 reported to the IT department by Point of Contact. After taking necessary corrective action IT department should inform PoC about the same, so that the port can be turned on by them.

G. Rebuilding the computer system

When the IT department reformat the computer systems and re-install OS and other application software, care should be taken to give the same host name, 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/ technical team 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 IT Department

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

13.3. Responsibilities of User/Department/Section/Institutes/Schools/Units/Centres/Hospitals

1. User Account

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

Once a user account is allocated for accessing the NitteDU's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the NitteDU 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 NitteDU community, when using the NitteDU's network facilities and its user account, it becomes user's utmost duty to respect the NitteDU's reputation in all his/her electronic dealings within as well as outside the NitteDU. It is the duty of the user to know the IT policy of the NitteDU and follow the guidelines to make proper use of the NitteDU's technology and information resources.

2. Logical demarcation of institutes, units, centres or schools network.

In some cases, institutes, units, centres or schools might have created an internal network with in their premises. In such cases, institutes, units, centres or schools assumes responsibility for the network service that is provided on all such internal networks on the institutes, units, schools, department or division side of the network backbone. The institute, department, section 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 institutes, units, centres or schools should identify at least one person as a Point of Contact(POC) and communicate it to IT department so that IT department can communicate with them directly in case of any network/system related problem at its end.

3. Supply of information by departments, sections, institutes, units, centres or schools for publishing on /updating the NitteDU's web site.

All institutes/ units/centres/schools, /hospitals departments, or divisions should provide updated information concerning them periodically (at least before one week or earlier).

Hard copy of such information duly signed by the competent authority at departments, sections, institutes, units, hospital's centres or schoolslevel**,** along with a soft copy to be sent to the web master operating from

IT department. This policy is applicable even for advertisements/tender notifications published in newspapers, and the events organized by section, department, or division.

Links to any web pages that have to be created for any specific purpose or event for any individual Department Sections, Institutes, Units, Hospitals Centres, Schools or faculty can be provided by the web Coordinator upon receiving the written requests. If such web pages have to be directly added into the official web site of the NitteDU, 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 Web Coordinator well in advance.

4. Setting up of Wireless Local Area Networks/Broadband

A. Connectivity

i. This policy applies, in its entirety, to institutes, units, schools, hospitals, centres or departments wireless local area networks/broadband connectivity within the academic complex/ NitteDU premises premises. In addition to the requirements of this policy, institutes/ units/schools/ centres must register each wireless access point with IT department including Point of Contact information.

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

iii. Departments /Institutes/ Units/Schools/ Centres/Hospitals must secure permission for the use of radio spectrum from IT department prior to implementation of wireless local area networks.

iv. Departments /Institutes/ Units/Schools/ Centres/Hospitals 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 NitteDU IT Policy, setting up of such wireless networks should not be undertaken by the departments /institutes/ units/schools/ centres/hospitals without prior information to IT department.

5. Security:

In connecting to the network backbone, departments /institutes/ units/schools/ centres/ hospitals agrees to abide by this Network Usage Policy under the NitteDU 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.

6. Preservation of network equipment and accessories:

Routers, switches, fibre optic cabling, UTP cabling, connecting inlets to the network, racks, UPS, and their batteries that are installed at different locations by the NitteDU are the property of the NitteDU and are maintained by IT department.

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

- Removal of network inlet box.
- Removal of UTP cable from the room.
- Opening the rack and changing the connections of the ports either at jack panel level or switch level.
- Taking away the UPS or batteries from the switch room.
- Disturbing the existing network infrastructure as a part of renovation of the location. IT department 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.

7. Additions to the existing network

Any addition to the existing network done by departments/institutes/units/Schools/hospitals/centres or individual user should strictly adhere to the NitteDU's network policy and with prior permission from the competent authority and information to IT department.

NitteDU network policy requires following procedures to be followed for any network expansions as far as possible:

- 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.

8. 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.

9. Enforcement

IT Department periodically scans the NitteDU 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.

14. RESPONSIBILITIES OF THE ADMINISTRATIVE UNITS

IT Department needs latest information from the different administrative units of the NitteDU for providing network and other IT facilities to the new members of the NitteDU and for withdrawal of these facilities from those who are leaving the NitteDU, and also for keeping the NitteDU 's web site up-to-date in respect of its contents.

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

i. Information about new appointments/promotions.

ii. Information about super annuations / termination of services.

iii. Information of new enrolments.

iv. Information on expiry of studentship/removal of names from the rolls.

v. Any action by the NitteDU authorities that makes an individual ineligible for using the NitteDU's network facilities.

vi. Information on important events/developments/achievements.

vii. Information on different rules, procedures, facilities information related items nos should reach web coordinator 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 (by email) should be sent to IT department so as to reach the above designated persons.

15. 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 NitteDU standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of IT department.

2. All the computers should follow the standard naming convention

3. Guidelines for running Application or Information Servers:

A. Running Application or Information Servers

- Institutes/ Units/Section/Departments/Centres/Hospitals may run an application or information server.
- Individual faculty, staff or students on the NitteDU campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the NitteDU network.

B. Responsibilities for those running application or information servers:

Institutes/ Schools/Units/Sections/Departments/Centres/Hospitals may run an application or information server. They are responsible for maintaining their own servers.

- Application or information server content and services must follow content guidelines as described in NitteDU's guidelines for web Presence.

- Obtain an IP address from IT department to be used on the server

- Get the host name of the server entered in the DNS server for IP address resolution. NitteDU IT policy's naming convention should be followed while giving the host names.

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

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

- Operating System and the other security software should be periodically updated.
- Sections/Departments may run an application or information server provided they do the following:

    a. Provide their own computer, software and support staff

    b. Provide prior information in writing to IT department on installing such servers and obtain necessary IP address for this purpose. For general information to help you decide whether or not to run a department or organization web server, contact the IT department.

16. GUIDELINES FOR HOSTING WEB PAGES ON THE INTERNET/INTRANET

16.1. Mandatory practices

A. Provide the full Internet e-mail address of the web page maintainer.

B. Provide a link to the NitteDU home page from the parent (Department of origin) home page.

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

D. Maintain up to date pages. Proofread pages and test links before putting them on the web, and regularly test and update links.

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

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

16.2. Recommended practices

A. Provide information on timeliness (for example: August 2004; updated weekly; updated monthly, etc.)..

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

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

D. Indicate restricted access where appropriate.

E. Avoid browser-specific terminology.

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

G. Maintain visual consistency across related pages.

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

I. Keep home pages short and simple.

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

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

L. Maintain links to mentioned pages.

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

N. 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.

O. 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.

P. 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).

Q. Conform to accepted, standard HTML codes.

17. GUIDELINES FOR DESKTOP USERS

These guidelines are meant for all members of the NitteDU's Network User Community and users of the NitteDU network. Due to the increase in hacker activity on campus, NitteDU 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 ! $ % and * , . ? + - =

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. Do not leave password blank and

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

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

6. The guest account should be disabled.

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

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

9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks). When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

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

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

12. In addition to the above suggestions, IT department recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

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

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

18. GREEN COMPUTING

18.1. Overview and Purpose

Computers and other office machinery consume power and generate heat whenever they are on. employees should seek to optimize the power consumption of office machinery in order to reduce the waste, environmental impact, and energy costs associated with its use. Even small changes to the way we typically use and manage common devices can significantly reduce the amount of energy consumed by office machines. To help reduce NitteDU's carbon footprint, save costs related to energy consumption, and extend the life of computers and other equipment, NitteDU requires employees to follow energy efficient computing strategies for the devices for which they have direct responsibility. Moreover, we encourage employees to apply the same principles of energy conservation to shared use devices within office environments. This policy defines steps that employees should take to conserve the energy used by computers and shared use equipment.

18.2. Coverage

All employees, contractors, vendors, volunteers and other personnel who use, manage, or are responsible for the approval or procurement of computers and shared use equipment, including servers, network devices, office printers, copy machines, and fax machines.

18.3. Policy

A. Desktop (Personal) Computer Usage and Management

The configuration of desktop and laptop machines should be standardized so that power saving and/or energy management settings support energy efficient operation.

Computers should be configured to enact "sleep" or "hibernation" mode whenever the computer is not in use for more than one hour, or the minimum amount of time that does not impede typical work performance.

Turn off your computer monitor when it is not in use, such as during breaks, meetings, and other periods when you are away from your computer for more than half an hour.

Turn off peripherals, such as printers, PDA devices, fax machines, and scanners, when they will not be in use for more than three hours. Check with IT department to see if specific peripherals have "power saver" or "sleep" modes and configure devices to activate these modes at the minimal time that does not impede work performance.

If your desktop computer does not run processes overnight and is not scheduled for nightly backup, turn it off when you leave for the day. Plug computers and other equipment into power strips instead of wall outlets, which allows the equipment to be more easily turned off.

B. Shared Use Office Device Management

i. Use the "print preview" function for office applications to review documents before printing documents to public printers.

ii. Avoid printing email messages and other electronic documents unless you have a specific need to retain or distribute a hard copy.

iii. If printers allow two sided printing, use this option whenever possible.

iv. Use email or other electronic communication media whenever practical as an alternative to paper memos and faxes Copiers, faxes, and shared use office devices should be turned on only when needed.

v. On a daily basis, the first person who requires the use of a device should turn it on. Employees should turn off shared use devices at the end of each work day or, on a daily basis, at whatever time it becomes unlikely that the equipment will be used again before the next day.

C. Development, Architecture, and Infrastructure Management

IT, project, and development managers should factor energy efficiency and utility cost savings into technology decisions. Visualization technologies that optimize server use, for example, can improve the operating efficiency of server and data centre environments. Development managers should consider the need for information availability in server allocation and selection. When possible, resources or processes that may be made periodically unavailable (e.g., overnight, on weekends, and over holidays) should be housed on servers that can be periodically shut down to reduce energy consumption.

D. Data Centre Management

i. The Systems Administrator must review and document data centre equipment use at least once in every two months for:

- Excess numbers of data copies, indicating inefficient use of server resources and dormancy of information resources stored in the data centre.
- Data that has not been accessed at least once in the previous one year should be marked for removal to offline storage media.
- Servers that do not support 24×7 operations and may be turned off after work hours, over weekends, and during holidays without interfering with normal business functions.

ii. In general, office and procurement managers should review equipment requests for energy efficient characteristics and seek energy efficient and/or green computing options for new purchases.

iii. Procurement should prefer equipment that is certified by the US Environmental Protection Agency's (EPA) “ENERGY STAR” program at a Plus 80 rating or higher.

iv. Where the cost difference between a technology alternative rated at Plus 80 is less than 10 percent higher than an alternative rated at a lower energy efficiency (all other factors being equivalent), the more efficient alternative should be purchased.

v. Laptop computers should be preferred over full sized desktop machines. This preference may be mitigated by factors of business use, user productivity, and organizational security policy.

vi. Flat panel liquid crystal display (LCD) monitors should be preferred over conventional cathode ray tube (CRT) monitors.

vii. Printers that can print on both sides of paper (duplex printing) should be preferred over single side printers.

viii. Except in cases of a specific business or security need for the procurement of a dedicated printer assigned to a single individual, departmental management and procurement should encourage the use of networked/shared printers.

ix. When procurement of a personal/dedicated printer is indicated, procurement should prefer more energy efficient inkjet printers over laser printers.

x. Procurement should actively seek and evaluate energy efficient and “green computing” offerings, noting computer vendors that offer resource efficient machines designed for eventual recycling.

E. Equipment Reclamation, Recycling, and Disposal Management

i. Employees who are not in charge of equipment disposal should not throw away computers or other equipment, even if they are non-functional. Employees should contact stores department to properly dispose of unused or unusable equipment.

ii. Employees who are responsible for equipment disposition should seek, whenever possible and always in compliance with secure disposal policies, to recycle, reallocate, or reuse reclaimed equipment.

iii. In cases where the entirety of a machine cannot be reused, stores department should seek to salvage and reuse any valuable components.

iv. CRT monitors contain hazardous materials and must be disposed of in compliance with Government of India’s Environment Policies Enforcement.

v. Wilful violation of this policy may result in disciplinary action which may include performance sanctions; termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student.

vi. Additionally, individuals are subject to restriction or suspension of the NitteDU’s email privileges, as well as civil and criminal prosecution.

19. VIDEO SURVEILLANCE POLICY

19.1.The system

19.1.1 The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; Digital recorders; SAN/NAS Storage; Public information signs.

19.1.2 Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

19.1.3 Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP camera installation is in use.

19.1.4 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

19.2. Purpose of the system

1. The system has been installed by NitteDU with the primary purpose of reducing the threat of crime generally, protecting NitteDU premises and helping to ensure the safety of all staff, students, patients and visitors consistent with respect for the individual's privacy.

These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

2. The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

3. Covert recording

Covert cameras may be used under the following circumstances on the written authorisation of BoardOf Management:

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

4. Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

5. The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

19.3.The Security Control Room

1. Images captured by the system will be monitored and recorded in the Security Control Rooms, "the control rooms", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

2. No unauthorised access to the Control Rooms will be permitted at any time. Access will be strictly limited to the duty controllers/officers, authorised members of senior management, police officers and any other person with statutory powers of entry.

3. Staff, students and visitors may be granted access to the Control Rooms on a case-by-case basis and only then on written authorisation from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

4. Before allowing access to the Control Rooms, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

19.4.Security Control Room Administration and Procedures:

1. Details of the administrative procedures which apply to the Control Rooms will be set out in a procedures manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

2. Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisors is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the procedures manual.

19.5.Staff

All staff working in the Security Control Rooms will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisors will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

19.6.Recording

1.Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

2. Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the log will be updated accordingly.

3. All hard drives and recorders shall remain the property of NitteDU until disposal and destruction.

19.7.Access to images

1. All access to images will be recorded in the access log as specified in the procedures manual

2. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

3. Access to images by third parties:

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

4. Access to images by a subject:

CCTV/IP camera digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. /IP camera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

a.A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 9 AM to 01 PM Monday to Saturday, except when NitteDU is officially closed or from the Data Protection Officer, the Records Office during the same hours.

b. The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the NitteDU Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

c. The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

d. All such requests will be referred to the Security Control Room Supervisors or by the Data Protection Officer.

e. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

19.8.Request to prevent processing

1.An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

2. All such requests should be addressed in the first instance to the respective Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

19.9.Complaints

It is recognised that members of NitteDU and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke NitteDU's Centralised Complaints Procedure by obtaining and completing a NitteDU Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Systems Administrator. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, these rights do not alter the existing rights of members of NitteDU or others under any relevant grievance or disciplinary procedures.

19.10.Compliance monitoring

A. The contact point for members of NitteDU or members of the public wishing to enquire about the system will be the Security Office which will be available during the working hours from Monday to Saturday except when NitteDU is officially closed.

B**.** Upon request enquirers will be provided with:

A summary of this statement of policy

An access request form if required or requested

A subject access request form if required or requested

A Copy of the NitteDU Central Complaints Procedures

C. All documented procedures will be kept under review and a report periodically made to the Board of Management through the Registrar-NitteDU.

D.The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Board of Management through Registrar- NitteDU.

20. APPENDIX

20.1. 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 Access ID (user account)/email account, you agree to act in accordance with the IT policies and guidelines of NitteDU. 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 NitteDU User can have a copy of the detailed document from the Intranet (viz. **http://nitte.edu.in**).

A Net Access ID is the combination of a user name and a password whereby you gain access to NitteDU computer systems, services, campus networks, and the internet.

1. 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 NitteDU. Students, staff and faculty who leave the NitteDU will have their Net Access ID and associated files deleted (After approval from HR Section and IT department). 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.

2. Limitations on the use of resources

On behalf of the NitteDU, IT department 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.

3. Computer Ethics and Etiquette

The User will not attempt to override or break the security of the NitteDU 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 NitteDU policy and applicable. Electronically available information.

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

(b) may not violate NitteDU policy prohibiting sexual harassment,

(c) may not be used for commercial purposes,

(d) should not appear to represent the NitteDU without appropriate permission, or to represent others,

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

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

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

(i) 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. IT department equipment does not support use of scripting in individual pages.

4. Data Backup, Security, and Disclaimer

IT department 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 IT department staff member in the process of helping the user in resolving their network/computer related problems. Although IT Department 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, IT department 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 IT department as part of NitteDU, harmless for any such liability or expenses. NitteDU retains the right to change and update these policies as required without notification to the user.

5. Account Termination and Appeal Process:

Accounts on NitteDU 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, IT department will make an attempt to contact the user (at the phone number they have on file with IT department) 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 IT department of the same, but, if the termination of account is on the grounds of wilful breach of IT policies of the NitteDU 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 Head of IT department, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Registrar/ appeal board duly constituted by the NitteDU 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 NitteDU'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 beforeVice Chancellor for further actions.

Policy Supporting Documentation	**Policy Support Contact**
Service and Conduct Rules	Systems Administrator
NITTE (Deemed to be University)	NITTE (Deemed to be University)