IT Policy

PREAMBLE

NIILM University Information Technology (IT) Policy sets forth the policies that govern the responsible usage of all users of the University's information technology resources. This comprises the IT facilities allocated centrally or by individual departments. Every member of University is expected to be familiar with and adhere to this policy. Users of the campus network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others.

Applicably

The IT Policy applies to all University faculty, staff and students and all others using the IT resources, whether personally or of University owned, which access, transmitter store various types of related information.

Objectives

Each user of the University Information Resources must ensure that it is used for promoting the mission of the University towards teaching, learning, research, and administration. In particular, the major objectives of this document are:

✓ To ensure the integrity, reliability, availability, and superior performance of the University IT Systems.
✓ To ensure that the IT resources protects the official e-identity (allocated by the University) of an individual.
✓ To ensure that all the users of the University are responsible for adhering to the procedures governing the implementation of this Policy document and any other matter incidental to those rules.

Need for IT Policy

Basically, the University IT policy exists to maintain, secure, and ensure

• Legal and appropriate use of Information technology infrastructure established by the University on the campus. This policy establishes University-wide strategies and responsibilities for

• Protecting the Confidentiality, Integrity and Availability of the information assets that are accessed, created, managed and or controlled by the University. Information assets addressed by the policy include data, information

• Systems, computers, network devices, intellectual property as well as documents and verbally communicated information]

Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, Govt. VYT PG Autonomous University took initiative way back in 2015 and established basic network infra structure in the academic complex of the University.

Over the last six years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the University's academic environment. Now, the University has about 30 network connections covering twenty five departments across the campus. All the faculty members using this network for teaching and learning

NIILM University is getting its Internet band width from BSNL. Total band width availability from BSNL source is 100 Mbps. While educational institutions are providing access to Internet to their faculty, students, and staff, they face certain constraints:

- Limited Internet band width.
- Limited infrastructure like computers, computer laboratories
- Limited financial resources in which faculty, students and staff should be provided with the network facilities.
- Limited technical man power needed for network management.

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

At the outset, we need to recognize the problems related to uncontrolled surfing by the users:

- Prolonged or intermittent surfing, affecting quality of work.
- Heavy down loads that lead to choking of available band width.
- Confidential information being made public.
- With the extensive use of the Internet, network performance suffer sin three ways:
- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.
- When users are given free access to the Internet, non-critical downloads may clog the traffic, result in gin poor Quality of Service (QoS) and affecting critical users and applications. When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.
- Too many concurrent users who are on the high-speed LANs trying to access Internet resources through a limited band width, create stress on the Internet band width available.
- Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files IT POLICY NIILM University are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate them selves, taking up network space and slowing down the network. Apart from this, plenty of employee time is lost with a work station beings canned and cleaned of the virus. Emails, unsafe download, file sharing and web surfing account for most of the virus attacks on networks.

Once they enter the network, viruses attach them selves to files, replicate quickly and cause untold damage to information on the network. They can slow down or even bring the network to

halt. Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So, pre venting it at the earliest is crucial. Hence, to securing the network, Internet Unit has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified, and infringing the freedom of users. As IT users are aware, all the educational institutions worldwide have IT policies implemented in the irrespective institutions. Without strong management policies, IT security measures will not be effective and not necessarily aligns with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are assign of due diligence, often necessary in the event of an IT audit or litigation. Policies also serve as blue prints that help the institution imp lament security measures. An effective security policy is as necessary to a good information security program as a solid foundation to the building.

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

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing requirements of the IT user community, and operating procedures. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of University community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies.

AREAS

IT USAGE AND PROHIBITIONS

- ➤ The users of the University shall make effective usage of campus collaboration systems, internet, wireless resources, official websites (including University website, conference website, journal portals, online admission systems, and course website), and Management Information Systems (MIS) and ERP solutions, Learning Management System, Remote Login based facilities of the University and e-Library resources.

- ➤ The University shall stress upon the users to comply with University policies and legal obligations (including licenses and contracts).

- ➤ The University shall strive to arrange for awareness programmes to acquaint the users with the effective usage of IT resources.

- ➤ **Prohibited Use** - The users shall not send, view, or download fraudulent, harassing, obscene,

threatening, or other messages or material that are a violation of applicable law or University policy. Contributing to the creation of a hostile academic or work environment is prohibited.

- **Copyrights and Licenses** - Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file sharing using the University's information resources is a violation of this policy**.**

- **Social Media** - Users must abide by the rules of the University towards the usage of social networking sites, mailing lists, news rooms, chat rooms and blogs.

- **Commercial Use** - The University IT resources shall not be used for any commercial and promotional purposes, through advertisements, solicitations or any other message passing medium, except as permitted under University rules.

SECURITY AND INTEGRITY

- **Personal Use** - The University IT resources should not be used for activities violating the basic functionality and mission of the University, except in a purely incidental manner.

- The users must refrain from making any unauthorized access of information to promote secure access of Network and Computers.

- The competent system administrator may access the information resources for a legitimate purpose.

- **Firewall** - Additional procedures to maintain a secured flow of internet and intranet-based traffic in the campus shall be managed through the IT POLICY VYTPG AUTO. UNIVERSITY DURG use of Unified Threat management (firewall).

- **Anti-virus and security updates** - The regular updating of the anti-virus policy and security updates should be done for the protection of computing resources.

IT ASSET MANAGEMENT

- **Asset Management**: The University shall lay down processes for the management of hardware and software assets that facilitates the usage of IT resources in the University. This shall include procedures for managing the purchase, deployment, maintenance, utilization, energy audit, and disposal of software and hardware applications within the University.
- **Copying and Distribution**: The University shall ensure that there is no violation in the copying and distribution of proprietary and licensed softwares.
- **Risks:** The University shall emphasize on managing the risks involved for the usage of IT resources. This shall include standard procedures for identification, minimization, and monitoring of risk impact by preventive and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate internet connectivity for a fail-safe internet access.
- **Open-Source Asset**: The University shall Endeavour towards the promotion and effective usage of open source softwares.

OPERATING ASPECTS

➢ **University Governance** - The University shall Endeavour to ensure fair-implementation of this policy to meet with the objectives of its formation. The responsibility of the management of operational aspects of IT resources is as per the hierarchical flow of the University governance structure.

➢ The respective Heads of the institutions shall be responsible for compliance with all University policies relating to the use/ownership of information resources, keeping in mind he Vision and Mission University.

➢ WEBSITE & TECHNOLOGICAL COMMITTEE at university level shall co-ordinate various activities related to the adherence of the IT policy is association with the respective institute.

➢ Individuals Users- The users are solely responsible for the activities tics they perform.1. on institute/University servers with their "User Name/Password and IP (internet Protocol)addresses assigned to them

VIOLATION OF POLICY

➢ Any violation of the basic objective and areas mentioned under the IT policy of the University shall be considered as a violation and as a misconduct and gross misconduct under University Rules.

IMPLEMENTAT1ON OF POLICY

➢ For implementation of is policy, the University will decide necessary rules from time to time.

REVIEW AND MONITORING

➢ The policy document needs to be reviewed at list once in two years and updated if required, to meet the pace of the advancement in the IT related development in the industry.