



## **INFORMATION TECHNOLOGY POLICY**

### Need for IT Policy

- Basically the KIAMS IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the KIAMS on the campus.
- This policy establishes KIAMS-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 KIAMS.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, KIAMS took initiative way back in 2000 and established basic network infrastructure in the academic complex of the university.

Over the last ten 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 2500 network connections covering more than twenty buildings across the campus and expected to reach 4000 connections very soon.

Internet Unit is the department that has been given the responsibility of running the university's intranet & Internet services.

Internet Unit is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university.

KIAMS is getting its Internet bandwidth from Airtel and Reliance Jio. Total bandwidth availability from each source is 50 Mbps (leased line).



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

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

On one hand, resources are not easily available for expansion to accommodate the continuous rise in Internet needs, on the other hand uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes nor governance of the 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 downloads that lead to choking of available bandwidth
- Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.
- Confidential information being made public.

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

- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.
- When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

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



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

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

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

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

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

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

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation.

Policies also serve as blueprints that help the institution implement security measures. An effective security policy is as necessary to a good information security program as a solid foundation to the building.



Hence, KIAMS 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 IT Technology (IT)". Hence, this document makes an attempt 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 technology, changing requirements of the IT user community, and operating procedures.

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

Guidelines are created and provided to help organisation, departments and individuals who are part of university community to understand how KIAMS policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- KIAMS Database Use Policy

Further, the policies will be applicable at two levels :

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

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



or by authorised resident or non-resident

visitors on their own hardware connected to the university network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognised Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the university.

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 university IT policy.

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the KIAMS's information technology infrastructure , must comply with the Guidelines. Certain violations of IT policy laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.