



RKDF University
Gandhi Nagar, Bhopal

IT Policy & Guidelines (Revised)

Approved in Board of Management on 07/08/2018

And by governing body on 11/09/2018


Registrar
RKDF University

(For official use)

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, servers, 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, The University took initiative way back in 2013 and established basic network infrastructure in the academic complex of the university.

Over the last Seven 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. Considering this change RKDF University decided to upgrade the network Infrastructure again in 2015.

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

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

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).
- When users are given free access to the Internet, non-critical downloads may congest 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 download, 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, Computer Center 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 guideline 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 necessary to a good information security program as a solid foundation to the building.

Hence, RKDF 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 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



Registrar
RKDF University

reflect changing technology, changing requirements of the IT user community, and operating procedures.

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

Guidelines are created and provided to help organization, departments and individuals who are part of university community to understand how University 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

Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, Senior administrators, Officers and otherstaff)
- 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 authorized 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, Laboratories, Offices of the university, hostels and guest houses, Teaching Departments 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.

Applies To

Stake holders on campus

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

Resources

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

1] IT Hardware Installation

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.


Registrar
KDF University

B. What are End User Computer Systems

Apart from the client PCs used by the users, the university 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.

C. Warranty

Computers purchased by any Section/Department/Project should preferably be with 1-year on-site comprehensive warranty. After the expiry of warranty, computers should be maintained by IT Department. Such maintenance should include OS re-installation and checking virus related problems also.

D. Power Connection to Computers and Peripherals


All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

E. Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.


Registrar
CDF University

G. 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 the record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room no. 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 Internet Unit of IT Department in writing/by email, connection will be restored.

H. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the Estate Branch, University IT Department will attend the complaints related to any maintenance related problems.

I. Noncompliance

The University 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 university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be non-compliant.

2] Software Installation and Licensing

Any computer purchases made by the individual departments/projects should make sure that such computer systems have licensed software (operating system, antivirus software and necessary application software) as well as free and open-source software (Linux, LibreOffice, LaTeX, etc.) installed.

Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances,


Registrar
RKDF University

university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for MS Windows and Linux 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 and Linux for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.
2. University as a policy encourages user community to go for open source software such as Linux, LibreOffice/OpenOffice to be used on their systems wherever possible.

B. Antivirus Software and its updating

1. Computer systems used in the university have anti-virus software installed, and it should be active at all times. Server is responsible for keeping the computer system compliant with this virus protection policy.
2. Server ensures that all respective computer systems have current virus protection software installed and maintained.

Server ensures that the software is running correctly. It may be noted that antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from IT department or any service-providing agency.



Registrar
RKDF University

3] Network (Intranet & Internet) Use

Network connectivity provided through the University. The IT department is responsible for the ongoing maintenance and support of the Network, inclusive of local applications.

A. IP Address Allocation

Any computer (PC/laptop/Server) that will be connected to the university network should have an IP address assigned by the 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 unauthorized from any other location.

Any IP base device like network printer, biometric machine, CCTV DVR, IP Camera, Video conferencing device etc. is to be installed at any location, then, the concern user should contact IT department and get proper IP Address.

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.

B. DHCP and Proxy Configuration by Individual Departments /Sections/Users

Use of any computer at end user location as a DHCP server or Wi-Fi router 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 university. 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 or creating Wi-Fi hot spots and connecting another computer to it is considered as proxy/DHCP configuration. Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.



KDF University

C. Running Network Services on the Servers

Individual departments/individuals connecting to the university 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 university IT policy for running such services. Non-compliance with this policy is a direct violation of the university 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 University 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 University'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 University Network connects. University 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 University Campus. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

D. Wi-Fi/Cellular/Leased Line Connections

Wi-Fi routers, switches, mobiles, Computer systems or any such devices that are part of the University's campus-wide network, whether university's property or personal property, should not be used for Internet connections, as it violates the University's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies, in its entirety, to Institute, department, or division wireless local area networks. In addition to the requirements of this policy, institute, departments, or divisions must register each wireless access point with IT Department including Point of Contact information.



Registrar
RKDF University