

Dr. B.N. Singh
Ph.D. (Austria) FNAVS
Registrar



Ph. : (O) 0755-2740395
(R) 0755 - 2759667
Mob. : 9713902378
Website : www.rkdf.ac.in
Email : drbnsingh@rkdf.ac.in

RKDF UNIVERSITY

(ESTABLISHED UNDER GOVT. OF M.P. AND APPROVED UNDER UGC 2(F) 1956)

No. **633/RKDF/2018**

Dated : **20/09/2018**

Notification

After the approval in the meeting of Board of Management dated 07.08.2018 and subsequent ratification by the Governing Body in its meeting held on 11.09.2018, the revised "IT Policy & Guidelines" is adopted and implemented with effect from the date of ratification by the Governing Body of the University.

A copy of the policy is enclosed herewith for kind perusal.

A handwritten signature in blue ink, likely belonging to the Registrar.

Registrar

Registrar
RKDF University

Enclosure: Revised IT Policy & Guidelines

Copy for information and for necessary action:

1. PA to Hon'ble Chancellor, RKDF University, Bhopal MP (for kind information)
2. Vice Chancellor, RKDF University, Bhopal MP
3. Exam Controller/CFAO/DSW, RKDF University, Bhopal MP
4. Dean/Institute Head, RKDF University, Bhopal MP
5. Notice Board, RKDF University, Bhopal MP
6. Website administrator, RKDF University, Bhopal MP
7. Office records

A handwritten signature in blue ink, likely belonging to the Registrar.

Registrar
RKDF University



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)


Registrar
RKDF University

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,

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 registered to

Registrar
RKDF University


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.

Registrar
RKDF University

Registrar
RKDF University

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

Registrar
RKDF 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
RKDF University


Registrar
RKDF 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


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.


Registrar
RKDF 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


Registrar
RKDF University

2. Institute, departments, or divisions must inform IT Department for the use of radio spectrum, prior to implementation of wireless local area networks.
3. Institute, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
4. If individual Institute wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Coordinator, IT Department.

F. Internet Bandwidth obtained by all Departments

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

G. Internet Access

Normally Internet access is available to all computers, laptops, servers, mobile devices and other IP based devices which are authorized to connect to the campus network.

It is responsibility of the individual to access Internet in the ethical and legitimate manner. Sometimes the user is unaware of risks in accessing some websites/web applications/apps and may get infected with virus, malware, adware or expose vulnerability. Therefore, users are broadly categorized as faculty, research students, UG/PG students, officers, clerical staff and technical staff. Depending on the category Internet access will be filtered at firewall. So, that intentional or unintentional access to


Registrar
RKDF University


Registrar
RKDF University

malicious websites/web applications (eg. Gaming, streaming, social media, online shopping etc.) will be avoided by default.

In case a website is filtered out, however it is essential for academic and administrative purpose, then the individual/ section/ department may request to Internet Unit. After verifying the need, authenticity and safety, Internet Unit will make the requested website available. (eg. Banking sites, payment sites, and temporary links on Government sites etc.)

H. Wi-Fi implementation and usage

Applies to

Stake holders on campus or off campus

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

Resources

- Wi-Fi Access Points /routers installed by University
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Multimedia Contents

Wi-Fi facility is implemented for the above mentioned stake holders in the campus.

For uniform and efficient and solicited usage of the Wi-Fi facility policies are defined as follows:

Wi-Fi Access and locations

1. Wi-Fi Access Point Location: Almost all buildings in the campus have been built using stones. Therefore implementing Wi-Fi facility was a great challenge.

Making Wi-Fi available in every room will not be economic. Furthermore, it was suggested that Wi-Fi facility may be made available in mostly at common places like canteen, library, hostel corridors, department corridors, Laboratories etc.

2. Wi-Fi Access Points may not be placed in the classroom.
3. Wi-Fi Access Points may be placed temporarily on demand in auditoria and other places, for conference, workshops, symposia and any other important events.
4. Personal Wi-Fi Access devices may not be allowed; as such devices may cause disturbance in IP allotment and security threat to University's Network. If found the personal devices may be confiscated by IT department.
5. In special cases the individual or department may approach to Internet Unit and get proper secure configuration and registration of the personal/ department's Access Points or routers.

Wi-Fi Usage

1. The individual user will be responsible for his/her Wi-Fi usage made.
2. Solicited and ethical usage is expected from the users.
3. The Internet Access through Wi-Fi is filtered access. Possible phishing, spurious, unsolicited or obscene sites, gaming sites, some shopping/multimedia streaming site are blocked at firewall level.
4. The users will access the University Resources properly and will not try to harm the resources.

Misuse and actions

1. If a user or his/her device is making any harm to university resources or other users, then such a user will be warned by Internet Unit. User's intention and device are verified. The corresponding Head of the department will be informed accordingly.
2. A virus infected device may create noticeable network traffic or attempts cyber-attacks. Then the user will be notified and his/her access shall be blocked until the infected device is cleaned/ free from viral infection.
- 3.



Registrar
RKDF University


Registrar
RKDF University

4] Email Account Use

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University 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 <https://www.rkdf.ac.in:2096> with their User ID and password. For obtaining the university's email account, user may contact IT department for email account and default password by submitting an application in a prescribed format. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. Institutional email facility should be used primarily for academic (such as researchgate, academia, arXiv etc.) and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and


Registrar
RKDF University


Registrar
RKDF University

suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have potential to damage the valuable information on your computer.

6. Users may configure messaging software (Outlook Express/ Mozilla Thunderbird messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
7. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the university IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Gmail, Hotmail.com, Yahoo.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

Registrar

RKDF University

Registrar
RKDF University

5] Web Site Hosting

A. Official Pages

Sections, departments, and Teachers/Employees/Students may have pages on RKDF's Intranet Channel of the official Web page. Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting. As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., <https://www.rkdf.ac.in> only.

B. Web Pages for eLearning

Faculties 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 University's Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official University or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

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

Servers:

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

Maintenance:

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

C. Network Protocol Access

As a standard practice HTTP, HTTPS, FTP, SMTP, DNS are the protocols available to all users in the campus. In case a genuine website is hosted on some other protocol or port, then the user/ section / department may inform the Internet Unit. After verifying the need, authenticity and safety, Internet Unit will make the requested website and protocol available.

For academic or administrative work some web applications hosted on the University servers. Such web applications should be hosted on standard HTTP and/or HTTPS ports only.

Acceptable Usage Policy (RKDF University)

Following is a brief summary of relevant University policies regarding computer and network usage. All policies in their entirety can be found on the University's website or requested from the University IT Department.

Acceptable Use Policy: University information technology resources, including electronic communications on the campus and the computers attached to this network, are for the use of persons currently affiliated with University, including faculty, staff and students. Information technology resources are provided by the University to further the mission of e-governance and lifelong education. Use of these resources should be consistent with this mission and this policy. Central to appropriate and responsible use is the stipulation that computing resources shall be used in a manner consistent with the instructional, public service, research, and administrative objectives of the University. Use should also be consistent with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use and may jeopardize further access to services.

This Acceptable Usage Policy covers the security and use of all information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all employees, Students, Guests, Temporary Employee's, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to academic and administrative activities worldwide, and to all information handled by relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by or on its behalf.

Unacceptable uses include, but are not limited to, the following:

- Using the resources for any purpose that violates University/State Act.
- Using the resources for commercial purposes, sales and/or advertising.
- Using excessive data storage or network bandwidth in such activities as propagating

Registrar
RKDF University

Registrar
RKDF University

of “chain letters” or “broadcasting” inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages.

- Sending or storing for retrieval patently harassing, intimidating, or abusive material.
- Misrepresenting your identity or affiliation in the use of Information Technology resources.
- Using someone else’s identity and password for access to information technology resources or using the network to make unauthorized entry to other computational, information or communications devices or resources.
- Attempting to evade, disable or “crack” password or other security provisions of systems on the network.
- Reproducing and/or distributing copyrighted materials without appropriate authorization.
- Copying or modifying files belonging to others or to the University without authorization including altering data, introducing or propagating viruses or worms, or simply damaging files.
- Interfering with or disrupting another information technology user’s work as well as the proper function of information processing and network services or equipment.
- Intercepting or altering network packets.

Computer Access Control – Individual’s Responsibility

Access to the IT systems is controlled by the use of User IDs, passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else’s user ID and password to access IT systems. Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to IT systems or information. Attempt to

Registrar
RKDF University

Registrar
RKDF University

access data that they are not authorized to use or access.

- Exceed the limits of their authorization or specific Academic and Administrative need to interrogate the system or data.
- Connect any non-authorized device to the network or IT systems.
- Store data on any non-authorized equipment. Give or transfer data or software to any person or organization. Outside without prior permission from authorities.

Internet and email Conditions of Use

Use of internet and email is intended for Academic and Administrative use. Personal use is permitted where such use does not affect the individual's Academic and Administrative performance, is not detrimental to in any way, not in breach of any term and condition of employment and does not place the individual or in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal Academic and Administrative.
- Use the internet or email for share marketing, auctions, gamble etc.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to, alter any information about it, or express any opinion about, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Forward mail to personal email accounts (for example a personal Gmail, Hotmail account).


Registrar
RKDF University


Registrar
RKDF University

- Make official commitments through the internet or email on behalf of unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect devices to the internet using non-standard connections. Like external USB Modem, Mobile Devices, Jio Wi-Fi etc.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, enforces a clear desk and screen policy as follows:

- Personal or confidential Academic and Administrative information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All Academic and Administrative-related printed matter must be disposed of using confidential waste bins or shredders.

Registrar

RKDF University

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data

Individuals must not

Registrar
RKDF University

Store personal files such as music, video, photographs or games on University IT equipment. i.e. Servers and Storage Equipment's

Viruses

The IT department has implemented centralized, automated virus detection and virus software updates within the University. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved anti-virus software and procedures.
- Install Anti-virus solution from any other brand/product (unauthorized / not licensing)

Telephony (Voice) Equipment Conditions of Use

Use of voice equipment is intended for Academic and Administrative use. Individuals must not use voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non- urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use voice for conducting private Academic and Administrative. Make hoax or threatening calls to Internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for Academic and Administrative use.

Actions upon Termination of Contract/Course completion/Service

- All equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to at termination of contract/Course completion/Service.


Registrar
RKDF University


Registrar
RKDF University

- All data or intellectual property developed or gained during the period of employment remains the property of and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

- All data that is created and stored on computers is the property of and there is no official provision for individual data privacy, however wherever possible will avoid opening personal emails.
- IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. University has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

It is individual responsibility to report suspected breaches of security policy without delay to IT Department through proper channel.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with disciplinary procedures.

Guidelines for running Application or Information Servers

Running Application or Information Servers

1. Section/Departments may run an application or information server.
2. Individual faculty, staff or students on the University 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 University network.

Responsibilities for Those Running Application or Information Servers

Sections/Departments may run an application or information server. They are responsible for maintaining their own servers.

- 1) Application or information server content and services must follow content guidelines as


Registrar
RKDF University


Registrar
KDF University

described in University Guidelines for Web Presence.

- 2) Obtain an IP address from IT Department to be used on the server
- 3) 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.
- 4) 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.
- 5) Operating System and the other security software should be periodically updated.
- 6) Sections/Departments may run an application or information server provided they do the following:
 - I. Provide their own computer, software and support staff
 - II. 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.

Guidelines for hosting Web pages on the Internet/Intranet.

Mandatory:

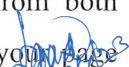
1. Provide the full Internet e-mail address of the Web page maintainer.
2. Provide a link to the University home page from the parent (department of origin) homepage.
- 3 Provide a link to the parent home page ("Return to department's home page") on all supporting local pages.
4. Maintain up to date pages. Proofread pages and test links before putting them on the Registrar Web, and regularly test and update links.
5. Know the function of HTML tags and use them appropriately.
- 6 Make provision for providing information without images as printer-friendly versions of the important web pages.
7. It is the responsibility of the concern department / section to keep the updated information on their webpages. All old information has to be removed from university website.

8. Each department / Section should visit daily to check their information on website.
9. In case of any RTI filed, then concern department / section has to reply to the concern applicant .
10. It is the responsibility of Website Cell to issue user-ID and Password to each department / section on request, they can modify their webpages but in case of any problem, Website Cell will help / modify the webpages.
11. It is the responsibility of Website Cell to host the given information from department / section on given webpage only. Responsibility of validity of information etc. lies with concern department / section only.

Recommended:

1. Provide information on timeliness
- 2 Provide a section indicating "What's New."
3. Provide a caution statement if link will lead to large pages or images.
4. Indicate restricted access where appropriate.
5. Avoid browser-specific terminology.
6. Provide link text that is clear without the link saying 'click here' whenever hyperlinks are used.
- 7 Maintain visual consistency across related pages.
8. Provide a copyright statement (if and when appropriate).
9. Keep home pages short and simple.
10. Avoid using large graphics or too many graphics on a single page.
11. Provide navigational aids useful to your users (Link to Home, Table of Contents, Next Page, etc.).
12. Maintain links to mentioned pages.
13. Make your Web pages easy to maintain for yourself and anyone who might maintain them in the future.
14. Avoid active links to pages that are in development. Place test or draft pages in your "test," "temp," or "old" subdirectory. Remember that nothing is private on the Internet: unlinked pages in your directory may be visible.
- 15 Check your finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended that you check your page


Registrar
KDF University


Registrar
RKDF University

with a Web validation service.

16. Think of your users--test with primary user groups (which will be mix of users linking through our high-speed network, and users linking via much slower modems).

17 Conform to accepted, standard HTML codes.

Guidelines for Desktop Users

These guidelines are meant for all members of the University Network User Community and users of the University network.

Due to the increase in hacker activity on campus, University 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 (K7 Enterprise Security) 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 and Linux 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.
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 should activate the built-in firewall.
8. All users should consider use of a personal firewall that generally comes along with the anti-virus software, if the OS does not have an in-built firewall.

Registrar
KDF University

Registrar
RKDF University

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.




Registrar
KDF University



Registrar
RKDF University

The University takes several quality initiatives were undertaken in the administrative domain in the post – accreditation period.

- Greater use of ICT for administrative purpose.
- Proposed Biometric attendance mode for all staff members.
- Augmenting the Admission part in the student module under the University website.
- The use of library management software (LMS) for Remote Login based facilities and e-Library resources.
- Installation of high vision CCTV for greater safety of students and staff member.


Registrar
RKDF University

Develop Smart Class Room for Purpose of On Line Classes.


Registrar
RKDF University