UNIVERSITY OF KASHMIR
HAZRATBAL, SRINAGAR

IT POLICY

POLICY STATEMENT

University of Kashmir expects all individuals using ICT resources of the university to take the appropriate measures for the efficient, economical and ethical use of all the IT resource provided to create, preserve, transmit and apply knowledge through teaching, research and creative works.

REASON FOR POLICY

The Purpose of this policy is present the various IT resources and services with respect to their usage, maintenance and security in order to establish the consistency in campus practice and process.
The term "resources" and "services" includes but not limited to computational resources (computers), networks (wired and wireless), servers, software systems, network access from off-campus, the gateway used for world wide web, e-mail, university portal, file tacking system , e-tutorial system, web page hosting and others.

Principles

1. The University's IT resources are maintained to support the work of the institution. The University reserves the right to monitor the use of these resources and to deal appropriately with users who use these resources contrary to the conditions of use set out in this policy.

2. The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources.

ENTITIES AFFECTED BY THIS POLICY

– All units of the university

WHO SHOULD READ THIS POLICY

– All members of the university community

WEB ADDRESS FOR THIS POLICY

http://www.kashmiruniversity.net/itpolicy

CONTENTS

I. Introduction

The purpose of this document is to inform members of the University of what can be expected in terms of Information Technology (IT). This covers the use of all computers and other related hardware such and the use of the network and software infrastructure. This policy document necessarily includes the Regulations and Policies applying to use of University ICT Facilities laid down by the University. In the following, the use of computers connected to the university network (main & off-campuses) both for academic and administrative purposes is covered together with the security policy and procedures.

II. Internet Policy

University of Kashmir provides all faculty, students, research fellows and staff with a modern, fully networked computing and IT environment for academic use.

Users of Kashmir University computing, networking and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve our right to access the international networks to which the system is connected. In case of complaints, appropriate action to be taken will be decided and taken by the Kashmir University Authorities.

Computers provide unequalled opportunities to explore and use a varied and exciting set of resources. In order to make these resources available to everyone, those who use the University's available technology must do so in a way that is consistent with their educational mission.

These rules are intended to provide general guidelines and examples of prohibited computer and Internet uses, but do not attempt to state all required or prohibited activities by users. Failure to comply with the Kashmir University Network and Internet Use Policy and these rules will result in loss of computer and Internet privileges, and/or legal and disciplinary action.

Guidelines for network users

1. Accounts & Passwords :

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else and it will only be used for educational/official purposes. The User guarantees that the Net Access ID will always have a password. Network ID's will only be established for Students and staff who leave the University will have their Net Access ID and associated files deleted.

Internet Policy , Continued

Employee Category	Number of Hours per day
Teachers (Permanent)	Unlimited
Teachers (Contractual)	8 Hours
Officers(Up to the level of SO)	Unlimited
Other Employees(Permanent staff below SO)	Unlimited with 2 Mbps
Temporary Employees (Contractual/Others)	8 Hours
Jr. Research Fellow	8 Hours
Sr. Research Fellow	8 Hours
Post Doctorate	8 Hours
Research Scholars	8 Hours
Students	4 Hours

No User will be allowed more than one Net Access ID at a time and one login is permitted at a time, with the exception that faculty or officers, who hold more than one portfolio, are entitled to have temporary Net Access ID related to the functions of that portfolio.

For Staff the validity for Net Access ID will be for one year and renewed on annual basis after re-verification. For students the validity for Net Access ID will be semester wise.

2. Limitation on use of internet resources :

On behalf of the University, Directorate of IT&SS reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

3. Computer Ethics & Etiquettes :

The User will not attempt to override or break the security of the University computers, networks, or machines/networks accessible therefrom. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk email messages comes under IT Policy violation.

User's Net Access ID gives him/her access to email, and campus computing resources. The use of these resources must comply with University policy.

The User:

a) Should not contain copyrighted material or software unless the permission of the copyright owner has been obtained.
b) Should not violate University policy prohibiting sexual harassment.

Internet Policy, Continued

c) Should not be used for commercial purposes.
d) Should not appear to represent the University without appropriate permission, or to represent others.
e) Should not appear to represent other organizations or companies.
f) Should not contain material which violates pornography laws, or algorithms or software which if transferred violate laws.
g) Should not contain scripts or code that could cause a security breach or permit use of resources in opposition to University policy.
h) Should not access TORRENT sites.

Unauthorized access to the KU wireless/Wi-Fi network using Network/RF devices by residents or employees residing nearby can lead to disciplinary action under rules against them and can lead to Fine of Rs. 50,000/- and lodge of F.I.R.

Wireless/ Wi-Fi access users need to immediately report to the Directorate of IT&SS if any incident or suspected incidents of unauthorized access point installation are noticed.

The University of Kashmir is not liable to provide internet access to the residential quarters or outside residential areas to any employees/staff or non-employee. However, if requested the service can only be made available on monthly payment basis for employees residing at University residential quarters and in no case free of charge. No employee residing in university residential quarters is entitled for free Internet access at their residences except the following:

i. Vice-Chancellor.
ii. Registrar.
iii. Controller Examination.
iv. Dean Academic Affairs.

The monthly tariff/charges applicable for Internet access to residential quarters shall be as under:

Plan	Bandwidth	Max. Data Limit	Charges/month
KU-20148	2048KB/s	25GB	Rs. 500/=
KU-4096	4096KB/s	35GB	Rs. 800/=
KU-5120	5120KB/s	45GB	Rs. 1200/=
KU-6144	6144KB/s	60GB	Rs. 1500/=

Internet Policy, Continued

Upon subscription by the respective employee, the above monthly tariff/charges shall be deducted (as per the plan opted by the user) every month from the salary. In case of any Wi-Fi equipment required for indoor use shall have to be provided by the user as per the specifications given by the Directorate of IT&SS.

4. Internet Connectivity to Hostels:

University shall provide the Internet connectivity to hostels for use of students/scholars. No extra Internet fee/charges shall be levied upon the hostel boarders for the same. However any theft of IT equipment installed in the hostels shall be deducted from the hostel boarders collectively.

5. Data Backup, Security, and Disclaimer:

Directorate of IT&SS will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an IT&SS staff member in the process of helping the user in resolving their network/computer related problems. In addition, Directorate of IT&SS makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold IT&SS, as part of Kashmir University, harmless for any such liability or expenses. The Directorate of IT&SS retains the right to change and update these policies as required without notification to the User.

6. Social Networking:

All Social networking sites are barred in the campus. Accessing such site through PROXY or by using special browsers will result in the deactivation of his/her NET Access ID. Also legal and disciplinary action will be taken against the rule violator.

7. Account Surrendering:

Retiring employees and the students leaving the university (temporarily or permanently) are advised to get their accounts (NET Access and Email) disabled by giving a written letter to Directorate of IT&SS. This is essential as the facility is meant only for the serving employees and the enrolled students. Further, in case the accounts are not disabled and misused by some unauthorized personals, the account holder would be legally responsible for such misuse of the account.

Internet Policy, continued

8. Account Termination & Appeal Process

Accounts on Kashmir University network systems may be terminated or disabled with little or no notice. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the Directorate of IT&SS of the same But, if the termination of account is on the grounds of willful breach of IT policies of the University by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she should approach the Director IT&SS, justifying why this action is not warranted.

Users should note that the University's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University authorities.

III. Information Security

The information assets of University of Kashmir are valuable to its objectives. The confidentiality, integrity and availability of University information assets are essential to the success of its operational and strategic activities. The University aims to secure its information assets by establishing an information security strategy that will enable the implementation of a robust information security risk management system and foster good security practices across its campuses.

The Information Security Policy is a key component of the University's Information Security Strategy built on a framework of information security management standards and best practices. The Information Security Policy will serve as an overarching policy document to provide a high level overview of information security management within the University.

The following principles govern the University's information security approach:

a) The University has adopted an information security risk management approach in line with the Institutional Risk Management Policy to ensure information security risk mitigation efforts reflect the University's risk appetite.
b) The Information Security Policy and supplementary policies, processes, standards, procedures and guidelines has been communicated to all users via training and awareness sessions, inductions, University intranet and internet, bulletins and other appropriate communication channels.

Information Security, continued

c) User access to the University's information assets will be based on job requirements rather than job titles. Access rights are reviewed at regular intervals and revoked if or where necessary.
d) The University believes that information security is the responsibility of its information asset users, and will set out the responsibilities for the strategic leadership, management and coordination of the information security strategy, and use of its information assets via relevant policies, job descriptions and terms and conditions of employments.
e) The University has established and promoted an information security awareness culture amongst its information asset users through user awareness and training, publications on information security risks and incidents, and guidelines for managing them.
f) Disaster recovery plans for mission critical information assets and related services have been established, tested and maintained.
g) The University has implemented an incident reporting and management system to enable prompt and appropriate incident resolution activities and inform risk assessments and management.
h) The University enforce and monitor compliance with the Information Security Policy, supplementary policies, processes, standards, procedures and guidelines. All users of University information assets must comply with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines and must also keep abreast of updates to these policies. Failure to adhere to the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be addressed by necessary disciplinary actions in accordance to the University's Staff Disciplinary Procedures, Student Disciplinary Regulations and Procedures.

IV. Network Security

All users of University information assets must comply with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines and must also keep abreast of updates to these policies. Failure to adhere to the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be addressed by necessary disciplinary actions in accordance to the University's Staff Disciplinary Procedures, Student Disciplinary Regulations and Procedures.
This policy applies to all members of the University of Kashmir community and authorized guests of the University:

a) Who connect network-capable devices to the Network (wired or wireless) on campus?
b) Who access resources or services that are located on the Network from off campus (their home or anywhere else on the Internet).

University students, instructors, researchers and staff are authorized to connect network-capable devices of an approved type to the Network. Instructors, researchers and staff may extend this authorization to guests on a temporary basis if they judge that so doing supports the University's mission, but in so doing they assume responsibility for their behavior. Authorization and access to the Network may be withheld or withdrawn with cause.

Network Security, continued

Only approved devices and device configurations are to be connected to the Network. Information about, and configuration requirements for approved devices will be maintained and provided by Directorate of IT&SS. Equipment that does not comply with these requirements should not be connected to the network. Exceptions to these requirements may be authorized to meet the academic needs of the University.

Any Department/Centre/Unit desiring to establish Wi-Fi at their respective departments need to take technical specification along with approved with approved configuration/make from the Directorate and devices purchased be informed and got configured from Directorate of IT&SS in order to ensure security on Wi-Fi devices.

Activities that interfere with the reliable operation of the Network are prohibited. These include, but are not limited to: operating network-capable devices that attack other network-capable devices, users of the Network and the Network itself; operating wireless access points, cordless phones and other devices using the unlicensed radio communications spectrum; and impersonating or interfering with Network equipment or Network services. Devices that interfere with the Network should be disconnected and/or removed.

Scanning and mapping the Network, as well as monitoring Network traffic, are prohibited unless authorized by Directorate of IT&SS.

The technical team of Directorate of IT&SS will scan devices connected to the Network for security issues and vulnerabilities. Network traffic are monitored to help ensure a reliable Network service and to protect Network users. Devices suspected to be in violation of this policy will be disconnected from the Network.

No Network/RF devices be installed on roof top of the building of Allama Iqbal library as well as anywhere in the campus without proper technical clearance /permission of the Directorate of IT&SS, failing which disciplinary action will be taken against the defaulter and the respective equipment's will be seized

V. Email Policy

Electronic Mail is a tool provided by the University and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of University Email Accounts evidences the user's agreement to be bound by this policy.

a) Directorate provides the email accounts to staff and research scholars on *uok.edu.in* or *kashmiruniversity.ac.in* domains on.
b) All staff, in particular administrative, academic and research staff should maintain and use only University email accounts and not use any external/personal account to conduct the official communications of the university.
c) The University's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments.
d) University employees' e-mail addresses are not confidential. Employee e-mail addresses will be visible to other University e-mail account holders.
e) E-mail sent by the University to a University e-mail account is an official form of communication to employees. It is the responsibility of employees and students to receive such communications and to respond to them as may be necessary.
f) Official Communications may be time-critical and employees and students are expected to review messages sent to their University e-mail account on a reasonably frequent and consistent basis.

Email policy, continued

General Standards of Use

E-mail facility provided by the University should not be used:

a) For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
b) for the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
c) For activities that violate the privacy of other users.
d) For the creation or transmission of anonymous messages, i.e. without clear identification of the sender.

VI. Risk Management

The University's Risk Management Policy is a high level document that sets out the University's approach for managing and reducing risks to an acceptable level.
In line with the Risk Management Policy, the University has developed an information security risk management system to support faculties and administrative offices in identifying internal and external risks to the security of the University's information assets they are responsible for. Relevant, appropriate and cost effective controls along with necessary training where applicable are implemented in a timely manner to mitigate identified risks.
In addition, the information security risk management system is a tool for evaluating the effectiveness of risk mitigation controls, and also informs the recommendation and implementation of new or additional controls where necessary, and ensures continuous monitoring of risks.

VII. Software Asset Management

The University of Kashmir is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative and service functions. The University's IT Acceptable Use Policy defines the acceptable behavior expected of users and intending users of the facilities, including the web facilities and systems. The University requires users to accept the IT policies and associated Requirements Governing the Use of IT Facilities as a condition of their use.
These are accessible on the University Policy Directory. These guidelines apply to all users of the university.
The following general principles apply to Software Asset Management.

a) It is the policy of the University of Kashmir to respect all software copyrights and license agreement terms/conditions that apply to University owned software installed on University and non-University owned IT facilities, or when used directly in support of its business operations.
b) IT facilities purchased with research and/or consultancy funds remain the property of the University of Kashmir and are treated as University owned IT facilities. Users should not duplicate any licensed software or related documentation for use either on University premises or elsewhere unless expressly authorized to do so under the prevailing software agreement.

Software Asset Management, continued

c) Users should not give licensed or copyrighted software to any external parties (including, but not limited to clients, contractors, customers), unless expressly authorized to do so under the prevailing software agreement.
d) Users should use software on local area networks, licensing servers, or on multiple machines only in accordance with the prevailing software agreement.

e) Assistance with software copyright or license arrangements can be obtained from the ITS Desktop Deployment Manager, the ITS Desktop Support Manager or the Software Asset Manager located in Directorate of IT&SS.

VIII. Green Computing

The University of Kashmir is committed to beneficial practices towards the community and seeks to benefit many stakeholders and constituencies. As part of this, the University endeavor to do no harm and curtail impacts on the environment, locally, regionally and globally. The University seeks to manage its Information Technology resources in ways consistent with those guiding principles and our mission imperative activity in teaching, research and service.

IX. Information Technology Service Management (ITSM)

IT Service Management (ITSM) is defined as a process-based practice intended to align the delivery of information technology (IT) services with needs of the business, which emphasizes benefits to users. IT Services embarked upon a path of implementing ITSM frameworks in early 2010 with the goal of establishing a common and convenient way for all faculty, staff, and students to interact with IT Services.