Jamia Hamdard

Policy Title- IT Policy		
1	**Policy Number**	JH/IQAC/PD-19
2	**Brief Description the Policy**	Students, Teaching and Non - Teaching Staff, Guests, and Research Scholars of JAMIAHAMDARD availing 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 and protect the privacy and work of students and faculty
3	**Scope/Objectives**	
4	**Policy Applies To (please tick)**	All academics (teachers and students) Administrative Managerial processes in the university
5	**Last Update**	September 03,2022
6	**Approved By**	Academic Council Board of Management
7	**Responsible Authority for Implementation and Monitoring**	Registrar, Head Computer Centre
8	**Superseding Authority**	Competent Authority/Body of the University
9	**References for the policy (please tick)**	NAAC accreditation NBA accreditation UGC/Govt. Directive

Policy statement

Jamia Hamdard committed to have IT as the medium for ensuring optimum dissemination of knowledge through its academic, non-academic pursuits and administrative service to all the stakeholders for the criterion of a knowledge society by molding the builders of future.

Students, Teaching and Non - Teaching Staff, Guests, and Research Scholars of JAMIA HAMDARD availing 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 and protect the privacy and work of students and faculty.

General Rules

- Students, Teaching and Non - Teaching Staff, Guests and Research Scholars are authorized to use the computing, networking, and other IT facilities for academic purposes, official university business, and for personal purposes if such use does not violate any law or any university policy.

- The Jamia Hamdard prohibits its users from gaining or enabling unauthorized access to forbidden IT resource on the University network. Any such attempt will not only be the violation of University Policy but may also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy and subject the user to both civil and criminal liability. However, the University reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

- The University prohibits its users from sending, viewing, or downloading fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable law or University policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g., when such content is received through e-Mail etc. As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

- Users must not violate Intellectual Property Right and Copyright Laws, and licensing policies with respect to copyrighted materials and software. Any unlawful sharing/use of any form of illegal or pirated or un-licensed software, on the University's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the Jamia Hamdard IT policy.

- University also recommends its students, faculty and office staff, to use Open-Source Operating Systems (OS) and Processing Software (PS) such as Ubuntu/ Centos or other and Libra Office/ OpenOffice/ WPS Office, respectively. Further, users of the computers sponsored directly or indirectly by JAMIA HAMDARD should migrate on the recommended OS & PS as their primary software and should generate expertise on it. In case of technical limitation in such adaptation, relaxation may be requested from

competent authority on valid grounds By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs, unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept ofdata privacy must be honored by each user.

- Users should not attempt to vandalize, damage, or change any data/information inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all the users at all the time. Any interference, disruption or encroachment in the University IT resources shall be a clear violation of the University policy.

- User should not attempt to affect the availability of IT resource, whether accidently or deliberately.

- Individual departments/sections and hostels etc. should retain consistency in compliance of the IT Policy, JAMIA HAMDARD, they may further define and implement additional "conditions of use" for IT resources under their control. It will be the responsibility of the Units to publicize and enforce such conditions of use. In cases where use of external networks is involved, suitable policies can be practiced in compliance with the broad prerogatives of Jamia Hamdard IT Policy.

- During certain investigation procedures, the University may berequired to provide its IT information, resource and/ or records, in parts or full, to third parties. Also, for proper monitoring and optimal utilization of University IT resources, the University may review, analyze, and audit its information records, without any prior notice to its users. Further, the University may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on theUniversity's IT resources.

- Users are supposed to take proper care of equipment and are expected to report any malfunction to the staff on duty or to the in-charge of the facility.

- Users should refrain from attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

- Consumption of food or drink is not permitted in the computer labs.

- Making noise either through games/music/movies or talking and/ or singing loudly in Computer labs is strictly prohibited.

- The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by means of e-mail, notices, or through the website.
- Any violation of IT Policy will be treated as misconduct. Depending on thenature of violation Jamia Hamdard may take appropriate action.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, Jamia Hamdard IT policy does not allow any pirated/unauthorized software installation on the JH owned computers and the computers connected to the campus network. In case of any such instances, Jamia Hamdard will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

Updated Antivirus Software

All Computer systems used should have anti-virus software installed, and it should be always active. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. When antivirus software that is running on a computer, which is not updatedor not renewed after its validity 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 Computer Centre

Email Account Usage Policy

To increase the efficient distribution of critical information to all faculty, staff and students 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 with their User **ID** and **password**. For obtaining the university's email account, user may contact Computer Centrefor email account and default password by applying in a prescribed form available at website.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The Email facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and facility may be withdrawn. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk email messages. And generation of threatening, harassing, abusive, obscene, or fraudulent messages/images.
- While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
- User should keep the mailbox used space within about 75% usage threshold, as 'mailbox full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- User should not open any mail or attachment from suspicious or unknown 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 important from the point of security of the user's system, as such messages may contain viruses that have potential to damage or steal the valuable and critical information on user's system.
- Users are advised to configure messaging software 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.
- Users 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.
- Users should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
- 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.
- Impersonating email account of others will be taken as a serious offence under the university IT security policy.
- It is ultimately everyone's responsibility to keep their e-mail account free from violations of university's email usage policy.

Social Media Policy

POLICY

- This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include What's App, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others.

PROCEDURES

- The following principles apply to professional use of social media on behalf of JAMIA HAMDARD as well as personal use of social media when referencing JAMIA HAMDARD.
- Employees need to know and adhere when using social media in reference to JAMIA HAMDARD.

- Employees should be aware of the effect their actions may have on their images, as well as JAMIA HAMDARD's Image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that The University may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to JAMIA HAMDARD, its employees, or stake holders.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment, or which may hurt religious & Sentiments of any one or any Community.
- Employees are not to publish post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Registrar's Office.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized University spokespersons.
- If employees encounter a situation while using social media that threaten to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of Registrar's Office.
- Employees should get appropriate permission before they refer to or post images of current or former employees, members, vendors, or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at JAMIA HAMDARD. The University's computer systems are to be used for official purposes only. When using University's computer systems, use of social media for official purposes is allowed only to those staff whose work profile requires use of social media (ex: Face book, Twitter and LinkedIn, What's app, Instagram, any other), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Subject to applicable law, after--hours online activity that violates or any other company policy may subject an employee to disciplinary action or termination.
- It is highly recommended that employees keep JAMIA HAMDARD related social media accounts separate from personal accounts, if Possible.
- Employees should not use any type of offensive /abusive language or make any comment/post any photo which is not appropriate.

Responsibilities of University Computer Centre

Maintenance of Computer Hardware & Peripherals

Computer Centre is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty or annual maintenance contract,and whose responsibility has officially been entrusted to it.

Complaints Management System

Computer centre may receive complaints from Network/WIFI Team, if any of the computer systems are causing network related problems.

Computer Centre may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in Computer Centre receives complaints from the users/ Network/WIFI Team of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

Scope of Service

Computer centre will be responsible only for solving the hardware related problems orOS or any other application software that were legally purchased by the university andwas loaded by the company.

Installation of Licenced Software

Computer Centre or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

Reporting IT Policy Violation Incidents

If Computer Centre or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the Network/WIFI Team and university authorities.

Network Operations

When the network port of any particular computer system is turned off due to virus orrelated activity that is affecting the network performance, the same will be informed to the Computer Centre by Network/WIFI Team. After taking necessary corrective action Computer Centre or service engineers should inform Network/WIFI Team about the same, so that the port can be turned on by them.

Rebuilding and reformatting the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files arealso downloaded from the net.

Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software filesfrom the infected hard disk dump should be used to write it back on the formatted harddisk.

Guidelines for System Users

These guidelines are meant for all members of the Jamia Hamdard user community and users of the Campus Wide Network.

Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen system security.

The recommendations are as follows:

1. All the computers should have the latest version of antivirus purchased by JamiaHamdard

And 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 betweenloss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, securitypolicies should be set at the server level and applied to the desktop machines.
3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for theadministrator account should be changed from the default.
4. The password should be difficult to break. Password, defined as:

- must be minimum of 6-8characters in length
- must include punctuation such as ! $ % & * , . ? + - =
- must start and end with letters
- must not include characters @ ' " `
- must be new, not used before
- Avoid using your own name, or names of your wife or children, or name of yourdepartment, or room No. or house No. etc.
- Passwords should be changed periodically
- All users are requested to make it a point to change default passwords given by the software at the time of installation

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 11 should activate the built-in firewall.
8. All users should consider use of a personal firewall that generally comes along the anti-virus software if the OS does not have an in-built firewall.
9. All the software on the compromised computer systems should be re-installed from scratch
10. Do not install Microsoft IIS or turn on any of its functions unless 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.

In addition to the above suggestions, Computer Centre 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 of data.

If a machine is compromised, Network/WIFI Team 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.