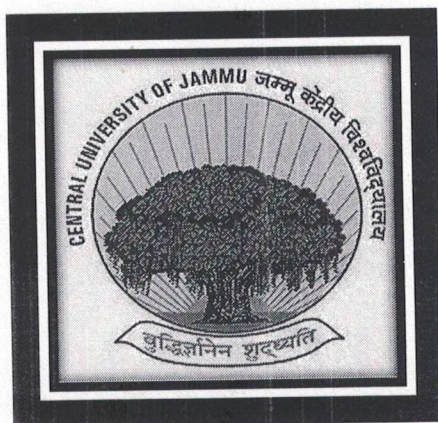


CUS/DIOA/AOAR-2019/37

26/06/2024

2019

Information Technology Policy Version 1.0



जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu


कुलसचिव
Registrar
जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu

Overview

This Policy applies to all Users of IT Systems, including but not limited to university students, faculty, and staff. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by ITS, as well as those administered by individual schools, departments, University laboratories, and other University-based entities.

Use of IT Systems, even when carried out on a privately owned computer or other device that is not owned, managed, or maintained by Central University of Jammu, is governed by this Policy. The University expects all employees, students and users to adhere to the policies herein. No set of policies can address all scenarios of IT security; therefore, these policies address the most common aspects of security. We cannot eliminate malevolent behaviour or irresponsibility, but we can guide users and administrators toward responsible decisions and actions.

Purpose

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. It will also ensure the ensure the legitimate and optimal use of IT resources at the university. Guidelines are created and provided to help organisation, 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 Content Updation Policy

Further, the policies will be applicable at two levels

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

Definitions

IT Systems

Any equipment or device that can store, process, or transmit electronic Central University Jammu data. This includes, but is not limited to, servers, personal computing devices, applications, printers, networks (virtual, wired, and wireless), supervisory control and data acquisition (SCADA) systems, building control systems (BCS), phones and cell phones, tablets, video surveillance equipment, radio equipment, routers, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by Central University of Jammu. For example, IT Systems include institutional and departmental information systems, faculty research systems, computer workstations and laptops, the University's campus network, and computer clusters.


कुलसचिव
Registrar
जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu

User

A "User" is any person, whether authorized or not, who makes any use of any IT System in Central University of Jammu from any location.

Systems Authority

While Central University of Jammu is the legal owner or operator of all IT Systems, it delegates oversight of particular systems to the head of a specific subdivision, department, or office of the University ("Systems Authority"), or to an individual faculty member, in the case of IT systems purchased with research or other funds for which he or she is personally responsible.

Systems Administrator

A person who is responsible for the upkeep, configuration, and reliable operation of computer systems, especially multi-user computers, such as servers. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to IT resources.

IT Hardware Installation Policy

IT Hardware Installation and Maintenance is performed by System Administrators / Senior Technical Assistant / Technical Assistants. Users need 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.

Faculty / Staff and the departments can submit IT Hardware requirements based on their academic / official requirements. Procurement of IT Hardware should be initiated based on the availability of stock and the requirements submitted by the departments. Stock Register should be updated immediately when IT Hardware is Procured. IT Hardware Installation and maintenance services are provided only after receiving an approval from the Competent Authority. Maintenance of Computer Systems should be done periodically by System administrators and the same need to be recorded in the Maintenance register. UPS should be used to connect all computers and peripherals to the electrical point. Since the UPS requires a continuous power supply to recharge its batteries, it is never recommended to turn off the UPS's power supply. These uninterruptible power systems (UPS) should also be connected to electrical points properly earthed and properly laid electrical wiring, among other requirements. Movement of IT Hardware within the university campus or outside the campus should be recorded in Movement Register. The Faculty / Staff or the Department is solely responsible for the IT Hardware provided to them and any damage or loss or theft need to be addressed by them only.

The major e-waste such as written off instruments /equipment's, Laptops, Printers, Computers, batteries should be sold regularly.

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, 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, university will hold the department/individual personally responsible



कुलसचिव
Registrar

जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu

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 all MS Windows 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 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, Open office to be used on their systems wherever possible.

3. Any MS Windows OS based computer that is connected to the network should access <http://windowsupdate.microsoft.com> web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates a being done properly.

B. Antivirus Software and its updating

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

2. 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. It may be noted that any 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 any service-providing agency.

C. Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool-proof solution. Apart from this, users should keep their valuable data on storage devices such as pen drives/ External Hard Disks.

D. Noncompliance

CUJ faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons


कुलसचिव
Registrar
जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu

An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even on whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

Network (Intranet & Internet) Use Policy

To use internet / Intranet services, Faculty, students and employees are provided user id, and passwords by the Digital Centre of Central University Jammu. Users are expected to respect the privacy of their fellow users and may not permit anyone else to use their password or share their account with them. The users 'responsibility is to protect their accounts from unauthorised use by changing passwords periodically and using passwords that are not easily guessed. The password needs to be at least 8 characters long with at least one special character and one uppercase. The sharing of passwords, for any reason, is strictly against the rules. The use of any method to circumvent system security, guess other people's passwords, or in any way gain unauthorised access to local or network resources is strictly prohibited. User accounts may not be used to access another person's computing account, nor may users attempt to forge an account identity or use a fictitious email address. Using the internet services provided by the University inappropriately or illegally by any user (whether a student or an employee) will subject the user to disciplinary action as determined appropriate by the competent authorities (including suspension or termination of Internet Services, imposition of an Internet Services fine, legal action, and other repercussions). All Internet / Intranet services provided by the University will be subject to periodic monitoring and surveillance to ensure that they are operating under university policies and procedures. Digital Centre of Central University Jammu reserves the right, on behalf of the University, to terminate the internet user id of any user who is deemed to be using excessive amounts of storage space or whose actions otherwise restrict the use of computing resources by other users.

E-mail Account Use 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.

Digital Centre will provide the email accounts to staff, students and research scholars on cujammu.ac.in domains. All staff, 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. The University's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments. University employees' e-mail addresses are not confidential. Employee e-mail addresses will be visible to other University e-mail account holders. 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. 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.


कुलसचिव
Registrar
जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu

Students Leaving the University

The Assistant Registrar Academics will provide the List of Students / Scholars to the Digital Centre, leaving the university so that such students email & Internet User account can be deleted.

Web Site Content Updation Policy

As a part of ongoing efforts to streamline and centralize content management, there is a Content Federation System (CFS) module for uploading all types of content on university official website. It helps to manage web content, allowing multiple contributors to create, edit, and publish the content on university official website. The CFS Portal module offers a user-friendly interface and ensures that all content is reviewed and approved before going live on the university website.

After Login in Samarth Portal, click on below mentioned steps

Data Management  **Content Federation System**  **Content**

The request to upload the content will reach to the Approver. Once approved by the approver, request will reach to the Publisher. The Publisher will publish the content on university official website.


कुलसचिव
Registrar
जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu
