Central University of Rajasthan

Information Technology Policy (IT Policy)

Central University of Rajasthan

NH8, Bandarsindri, Kishangarh, Ajmer 305817

Preamble

Central University of Rajasthan is committed towards sustainable development through efficient utilization of resources including Information and Communication Technology (ICT). Central University of Rajasthan is well connected with 1 Gbps broadband Internet connection as part of INFLIBNET. Every member of the university has access to the network and resources are available 24x7. The objective of this policy is to sensitize the users of IT in orderto avoid any mischief/misuse of the resources. This policy has been prepared and drafted in accordance to the Information Technology Act 2000 of Govt. of India. This policy is applicable to all the users of IT services in the Central University of Rajasthan.

Definitions

'**Computer**' means any electronic, magnetic, optical or any other high speed dataprocessing device or system that can perform arithmetic, memory and logical functions.

'**Computer System**' means a device or a group of devices that are programmable and can perform arithmetic, logical and memory functions.

'**Computer resource**' means a computer, computer system, computer network,data or software.

'**Computer Network**' means interconnection of one or more computers through some link like terrestrial cable, satellite, radio waves, micro waves, etc.

'**Data**' means collection facts, figures, statistics in any form.

‘**Information**’ means processed data including text, images, videos, audio files,software, databases, computer programs, etc.

‘**Electronic form**’ means data or record generated, stored, shared, transmitted indigital form.

‘**Access**’ means gaining entry to a computer, computer system, computerresource, computer network, data base, online resource, etc.

‘**User**’ means any person or a group permitted to can access the ITresources/infrastructure.

‘**Security procedure**’ is systematic process defined to provide/enhance securitylevel of an IT/ICT resource.

‘**Email**’ means communication method to deliver messages using electronicdevices.

ICT Cell

University shall have an ICT cell to leverage smooth functioning of university using IT, ICT cell shall be constituted for a period of 02 years and shall coordinatein rendering ICT services to the university community, it shall be headed by a teacher/officer and shall have members. ICT cell shall coordinate with the university in purchase and maintenance of IT related services. Convener of ICT cell shall convey the meetings and keep record of the minutes and recommendations done. All Technical/senior technical assistants shall be part of ICT cell and assist the university administration/ICT cell in rendering the IT services to the university community.

Hardware Installation Policy

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.

What are End User Computer Systems

Apart from the client PCs used by the users, the university will consider servers not directly administered by Computer Centre, 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 Computer Centre, are still considered under this policy as "end- users" computers.

Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite

comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

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, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

Network 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.

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.

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 Computer Maintenance Cell attached with Computer Centre will attend to the complaints related to any maintenance related problems.

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

Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so.

Use of software on Desktop systems

Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.

Any software installed should be for activities of the university only.

Antivirus Software and its updating

Computer systems used in the university should have anti-virus software installed, and it should be active at all times. 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.

Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

Security Incident Management Process

A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of University's data.

IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the university.

Web Administrator

Web administrator shall be appointed among the teachers especially fromComputer Science/CSE/Data Analytics departments to monitor design, updatingand maintenance of university website and online portals of the university. Theweb administrator shall also maintain the official email ids of university community.

Users

All the employees, students and visitors form the users of IT services of Central University of Rajasthan. The users need to strictly adhere to this IT policy and other regulations as defined by the government. Users are expected to use the IT services for academics, research, administration, or any other activity that is part or recognised as service to the university.

Computer as a resource

Every employee of the university whether regular, temporary, or outsourced shall be provided with a computer to accomplish their day-to-day activities. It isthe responsibility of the employee to up keep the computer provided and shall not involve himself/herself in the misuse of the computer. He/she shall be responsible to get the computer repaired/updated through ICT cell. Any loss ordamage to the computer shall be reported to the ICT cell and reporting officer immediately. An employee needs to surrender the computer or any otherstorage/printing device issued by university before relieving from the universityin working condition (unless was reported of damage or malfunctioning).

Email Ids

Official email ids shall be provided to every member of the university and all communications in electronic form shall be through official email ids only. An email sent or received through an official email id shall be official and the sender of the email shall be deemed to be the owner/creator of the message. He/she shall be held responsible for any outcomes of an email sent/circulated/forwarded through his/her email id. All the officials/teachers/students/staff of the university shall be provided with an official email id and any message received needs to be considered as official andlater the same message may be or may not be received on paper. A communication received through official email id shall be equivalent to the samecommunication received on paper in all the matters and circumstances.

Dos and Don'ts while using official email id:

1. Do not circulate any unauthorized or third-party content which you arenot fully aware of through official email id.
2. Official email id shall not to be used for personal communications.
3. Avoid forwarding the messages received from unknown sources usingofficial email id.
4. Do not open any link received from outsiders (unknown sources) onofficial email id.
5. Do not send/forward any message containing abusive/offending/anti-social content.
6. Do not use official email id for canvasing on your personal or illegitimateentities.

7. Do not use official email id to do any commercial transaction that is notofficial.
8. Report any mischief you identify regarding official email id to the webadmin immediately.
9. Do not use official email id to send messages related to any sensitive issueor for campaigning for an individual or a group.
10. Official email id is provided for official communications but not to formgroups and create discussion forums.

Restrictions and permissions to official email ids:

1. Hon'ble Vice Chancellor, Registrar, Librarian, Controller of Examinations, Chief Warden, Dean (Academics), Dean (Research), PS to VC, PS to Registrar, Proctor and wen admin are only permitted to send emails to a group. No other individual is permitted to send mails in groups.
2. Hon'ble Vice Chancellor shall have an email id created on his/her name apart from the official email id.
3. Email ids of students (UG and PG) shall be deactivated immediately after they complete their course and graduate from the university.
4. The email ids of PG students, whose course work involves research may be kept active for a period of 02 years from the time of their graduation on request.
5. The email ids of research scholars shall be kept active for a period of 5 years after their graduation.
6. The email ids of teachers/staff/officers leaving the university before 5 years shall be deactivated immediately, they leave the university. However, it may be kept active for some duration on request.

7. The email ids of teachers who leave the university after completing minimum 05 years of service shall be kept active unless requested to be deactivated.
8. Activating/deactivating an email id of a teacher/student/officer/staff shall be decided upon request by the competent authority.
9. The competent authority may deactivate an email id if it finds deemed tobe fit to do so.
10. Any misuse of email id by a former employee/student shall be immediately deactivated and it shall not be liable to be reactivated in anycase.

Internet Access:

Every member of the university is entitled to access Internet services through university Internet connection either through LAN or Wi Fi. Each such user shallbe provided a user id and password to get access of Internet services. The Internet services shall be restricted by a Firewall and the permissions shall be role based. It is strictly prohibited to access Internet services of the university for anti-social activities or any other activities restricted by government/university.The internet services can be accessed through Desktops/Laptops/Smartphones/Hand held devices. Any illegitimate activity done through university network is liable to be punished strictly. Users are strictly restricted from accessing anti-social/offending/porn content using university network, any such person found to be violating shall be strictlypunished. Users are advised to strictly adhere to the security procedures.

Online resources

The university subscribes to various online resources like e-journals, e-books, software's, tools, etc. and shall be accessible to the employees and students onneed basis. It is expected that the university community shall use these resources economically and for the benefit of the university community, university, society. It is not permissible to share these resources with persons/institutions/groups outside the university. Any violation of this may attract penalty.

Penalties

Any user indulging in violations of these policy or the regulations of the government shall be punished strictly. The punishment may range from deactivating the email id, blocking the user from accessing resources, or as decided the administration.