Policy for the Implementation and Application of Information Technology in Academic and Administrative Affairs of the University of Rajasthan

PREAMBLE

The University of Rajasthan is committed to sustainable development through the efficient utilization of resources including Information and Communication Technology (ICT). The University of Rajasthan is well connected with a high-speed 1 Gbps Internet connection as part of the National Knowledge Network (NKN). The Campus Wide Area Network (CWAN), named RUN (Rajasthan University Network), is based on Gigabit Ethernet Technology with Optical Fiber Backbone. It provides high-speed connectivity across the university campus, facilitating efficient communication and collaboration among students, faculty, and researchers.

The purpose of this policy is to ensure the legitimate and optimal use of IT resources at the university. The policy aims to facilitate safe, secure, effective, target-oriented, and lawful use based on the spirit of cooperation and sharing. The policy shall cover all Information Technology facilities and services provided by the University of Rajasthan. It shall regulate the use of ICT resources by all stakeholders, and IT facilities & information resources shall be the property of the University and not of a particular individual, School, or Centre. This policy has been prepared and drafted following the Information Technology Act 2000 of Govt. of India. This policy applies to all the IT services/resources users in the University of Rajasthan.

SCOPE

This policy shall be applicable for the use of information, electronic devices, computing devices, and network resources of the university. All students, employees, teachers, consultants, and other workers at the university are responsible for exercising rational judgment regarding the appropriate and judicious use of ICT infrastructure under the following:

- Policy and Guidelines on the Use of IT Resources & Devices and Subsequent Amendments/Modification

- IT Act 2000 including all subsequent Amendments
- E-mail, Password, and Security Policy of the Government of India
- Policy on adoption of Open-source Software
- National Cyber Security Policy-2013
- Guidelines for adoption of Electronic Payments and Receipt
- Policies and Guidelines issued by the National Knowledge Network (NKN) and CERT-IN
- Any other policy or guidelines issued by the Government of India and the Government of Rajasthan from time to time.

In addition to the above, the university can also devise guidelines for the expansion and use of ICT infrastructure. Such guidelines shall be open for amendments as and when required.

This policy applies to all members of the University community who utilize IT resources, including desktops, laptops, servers, tablets, smartphones, email accounts, and other IT hardware and software. It extends to IT resources owned or leased by the University, as well as those owned or leased by individual members of the University community used in connection with University activities.

DATE OF COMMENCEMENT

This policy shall be brought into force from the date of its approval by the statutory bodies of the University.

DEFINITIONS

Computer: An electronic device capable of performing arithmetic, memory, and logical functions.

Computer System: A programmable device or group of devices capable of performing arithmetic, logical, and memory functions.

Computer Resource: Any computer, computer system, computer network, data, or software.

Computer Network: The interconnection of one or more computers through various links such as terrestrial cables, satellites, radio waves, microwaves, etc.

IT Resources: Includes computer equipment, portable and mobile devices, network infrastructure (internet, intranet, wireless networks), external storage devices, peripherals (printers, scanners), software, and associated data and information generated for official purposes.

Network Resources: Any electronic/electrical and/or mechanical devices connected to the university's computer network.

User: Any individual or group permitted to access the IT resources/infrastructure.

Data: Collection of facts, figures, and statistics in any form.

Information: Processed data including text, images, videos, audio files, software, databases, computer programs, etc.

Access: Gaining entry to a computer, computer system, computer resource, computer network, database, online resource, etc.

Electronic Form: Data or records generated, stored, shared, and transmitted in digital form.

Email: A communication method to deliver messages using electronic devices.

Blog: A discussion or informational site published on the World Wide Web.

Malicious Program: Software designed to appear useful but gains unauthorized access to system resources or tricks users into executing malicious actions.

Security Procedure: Systematic process defined to provide/enhance the security level of an IT/ICT resource.

Disruption: Interruption or prevention of the correct operation of system services and functions.

Proprietary Information: Data or information that is part of official assignments and includes passwords or access credentials.

Competent Authority: Statutory body or designated official responsible for overseeing IT policies and procedures.

OBJECTIVES

The objective of this policy is to encourage the responsible use of IT resources in furtherance of the University's academic and administrative missions while safeguarding the confidentiality, integrity, and availability of information and IT resources.

ROLES AND RESPONSIBILITIES

All members of the University community utilizing IT resources are responsible for complying with this policy. The Infonet Centre is designated to enforce this policy and provide technical support and guidance to users of IT resources. It will oversee the wired and WiFi network as well as Internet connectivity within the university. Additionally, the Infonet Centre will manage the hosting, development, and maintenance of the University website and other web portals.

ACCEPTABLE USE

IT resources may solely be employed for legitimate University purposes and must not be utilized for illegal or unethical activities. Unacceptable use includes but is not limited to violating laws or regulations, engaging in activities harmful to others, interfering with the normal operation of the University's IT infrastructure, and participating in unrelated commercial activities.

OPEN SOURCE INITIATIVE

The University of Rajasthan advocates for the adoption of open-source software (OSS) that adheres to technical and security standards and aligns with University policies, consistent with the Government of India's open-source policy as part of the Digital India program. Free and Open Source Software (FOSS) empowers users to study, modify, and distribute the source code without royalty fees, promoting transparency and innovation. In contrast, proprietary software restricts access to the source code and imposes usage limitations.

The University promotes the use of open-source technologies, it recognizes that proprietary solutions may be necessary for specialized requirements or due to a lack of expertise. In such cases, exceptions may be considered with proper justification.

Departments and sections are required to include both OSS and proprietary software options in their procurement processes. Suppliers must justify any exclusion of OSS in their responses, with decisions prioritizing need, necessity, capability, security, and support requirements. Promoting the use of open-source solutions is encouraged due to their cost-effectiveness and flexibility.

DATA BACKUP, STORAGE AND SECURITY POLICY

- All data and software essential to the continued operation of the University, as well as all data that must be maintained for legal purposes, must be backed up.
- All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
- The application owner, together with the Infonet Centre, will determine what information must be backed up, in what form, and how often.

- The Registrar will be the sole authority of the entire digital data maintained and managed by the University.
- Concerned officials shall be responsible for the integrity and security of the data of that section.
- The University should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, to ensure segregation of duties and responsibilities, and to mitigate the risk of systems and data losses.
- Proper backup, storage, and handling of data are necessary for all departments. Staff must accurately follow the policy and protect the availability, confidentiality, and integrity of data.
- Critical data, which is critical to the University, must be defined by the Business in consultation with Infonet Centre and must be backed up.
- Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site). The medium will dictate the schedule.
- Data restores must be tested regularly.
- All data and software essential to the continued operation of the University, as well as all data that must be maintained for legal purposes, must be backed up.
- All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
- The application owner, together with the Infonet Centre, will determine what information must be backed up, in what form, and how often.

- The Registrar will be the sole authority of the entire digital data maintained and managed by the University.
- Concerned officials shall be responsible for the integrity and security of the data of that section.
- The University should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, to ensure segregation of duties and responsibilities, and to mitigate the risk of systems and data losses.
- Proper backup, storage, and handling of data are necessary for all departments. Staff must accurately follow the policy and protect the availability, confidentiality, and integrity of data.

- Critical data, which is critical to the University, must be defined by the Business in consultation with Infonet Centre and must be backed up.
- Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site). The medium will dictate the schedule.
- Data restores must be tested regularly.
- Before the adoption of any IT application developed by an external vendor, the vendor must provide a security audit certificate from a CERT-IN empaneled firm, ensuring compliance with established security standards and protocols.
- The servers designated for hosting the application and storing associated data must be located within the geographical boundaries of India, following data sovereignty and privacy regulations.
- Any data transmission or exchange between the university network and external servers must be encrypted using industry-standard encryption protocols to safeguard data integrity and confidentiality.
- Access controls and user permissions for the IT application must be implemented and managed effectively to prevent unauthorized access or misuse of sensitive information.
- Regular security assessments and vulnerability scans must be conducted on the IT application and associated infrastructure to identify and mitigate potential security risks and vulnerabilities.
- Incident response procedures must be established and documented to address any security breaches or incidents promptly, including notification protocols for affected users and stakeholders.
- Regular training and awareness programs on IT security best practices must be conducted for university staff and users to promote a culture of cybersecurity awareness and vigilance.
- Compliance with relevant regulatory requirements, such as data protection laws and industry-specific regulations, must be ensured throughout the lifecycle of the IT application, from procurement to decommissioning.
- Contracts and agreements with third-party vendors must include provisions for data security, confidentiality, and compliance with the university's IT policies and standards.
- Periodic review and audit of third-party IT applications and hosting infrastructure must be conducted to verify ongoing compliance with security requirements and address any emerging threats or vulnerabilities.

USE OF IT DEVICES ON RUN NETWORK

For connecting to Rajasthan University Network, the user shall ensure the following:

(a) Users intending to connect an IT device to the university network must register the device and obtain one-time approval from the Infonet Center.

(b) Upon request submission, the Infonet Center will assign a local IP address to the device. If a registered device is relocated to another network port without prior authorization, or if an unregistered device is connected to a network port, the port will be deactivated.

(c) Users are prohibited from utilizing VPN or similar software to circumvent the Proxy Server.

(d) All IT devices connected to the university network must adhere to established security protocols, including up-to-date antivirus software and firewall protection.

(e) Users are responsible for maintaining the confidentiality and security of their login credentials and must not share them with unauthorized individuals.

(f) Unauthorized access to or modification of network settings, configurations, or data is strictly prohibited and may result in disciplinary action.

(g) Users must report any suspected security breaches or incidents to the Imfonet Centre promptly.

(h) Network bandwidth usage must be reasonable and follow university guidelines. Excessive bandwidth consumption may result in network restrictions.

(i) Personal IT devices brought onto the university premises must comply with all IT policies and regulations.

USE OF IT DEVICES ON WI-FI NETWORK

For connecting to University of Rajasthan wireless, the user shall ensure the following:

(a) A user shall register the access device and obtain one-time approval from the Infonet Centre and submit an undertaking before connecting the access device to the wireless network.

(b) Wireless client systems and wireless devices shall not be allowed to connect to the wireless access points or remote network without due authentication.

(c) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

(d) The users shall be allowed to remotely access the services and resources of the University by adhering to the procedure to be notified and specified by the competent authority from time to time.

HANDOVER OF IT INFRASTRUCTURE PROVISION

(a) The handover of IT infrastructure provision must follow a documented and structured process, including comprehensive documentation of system configurations, network architecture, and user access controls.

(b) Before the handover, the outgoing IT personnel/officials must provide detailed instructions and training to the incoming staff regarding system administration tasks, user management, and maintenance procedures.

(c) User login credentials and official email passwords must be securely transferred to the responsible authorities or administrators designated to oversee IT operations following the handover process.

(d) It is strictly prohibited to delete or format any official computers or data storage devices before the handover. Any unauthorized data deletion or tampering will result in strict disciplinary action against the responsible individual(s).

(e) A thorough inventory of all IT assets, including hardware, software licenses, and peripherals, must be conducted during the handover process to ensure accountability and transparency.

(f) The incoming IT personnel/officials must conduct a comprehensive review of the existing IT infrastructure, including system configurations and security measures, to identify any gaps or areas for improvement.

(g) Proper documentation of the handover process, including signed acknowledgment from both outgoing and incoming IT personnel, must be maintained for audit and compliance purposes.

(h) Any changes or modifications made to the IT infrastructure post-handover must adhere to established change management procedures and receive appropriate authorization from designated authorities.

THE MODALITIES FOR GENERAL USE, ACCESS TO NETWORK, AND OWNERSHIP

- The proprietary information of the University stored on electronic and computing devices whether owned or leased by the university, the employees, and students, or a third party remains the sole property of the University of Rajasthan.
- The users of IT facilities and services of the university shall be responsible for promptly reporting the theft, loss, or unauthorized disclosure of the University's proprietary information.
- The users shall access, use, or share the University of Rajasthan proprietary information only to the extent it is authorized and necessary to complete the assigned job-related responsibilities.

FILTERING AND BLOCKING OF SITES

1. The university, through its Competent Authority, may block content on the Internet by issuing a circular, which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or policies of the University or which may pose a security threat to the network or undermine the interests of the university.
2. The university may also block content that, in the opinion of the Competent Authority, is inappropriate or may adversely affect the productivity of the users.

SECURITY AND PASSWORD

1. All IT resources shall be secured by strong passwords, including document as well as equipment passwords. The password should include a combination of lowercase & uppercase alphabets, numerical, and special characters.
2. All computing devices shall be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. The screen must be locked or logged off when the device is unattended.
3. PCs shall not be left unattended without logging off, and the user shall be responsible for any misuse of such a device by unauthorized access.
4. The users shall exercise utmost caution while opening e-mail attachments received from unknown senders, which may contain malware.
5. The users shall be responsible for all activity performed with their personal user ID and/or passwords. Permitting any other person to

perform any activity with one’s user ID and/or passwords shall be permissible with prior written approval from the competent authority with an undertaking that such a password shall be subsequently changed. These shall be treated as sensitive and confidential information.

6. No official of the University shall require, for whatever purpose, the password of other officials on any kind of questionnaire, in writing or oral, through phone or electronic message service unless permitted by the competent authority in writing with an undertaking that such a password shall be subsequently changed.
7. The users shall refuse all offers by the software to place a cookie on their computer so that they cannot automatically log on the next time when they visit a particular Internet site.

ELECTRONIC MONITORING

1. The university shall have the right to audit networks and systems at regular intervals, to ensure compliance with the policy in case of specific alleged misconduct or to redress any fault in the functioning of the system. However, this can be done on the prior approval of the competent authority and under intimation to the user.
2. The university or any person authorized on its behalf, for security-related reasons or compliance with applicable laws, may access, review, copy, or delete any kind of electronic communication or files stored on the devices under the possession of the university by adopting the following procedure:
   (a) The user must be intimated.
   (b) If found necessary to access or inspect any device without intimation to its user, it can only be done with the prior approval of the competent authority.

UNAUTHORIZED ACCESS

Any unauthorized access to any system or its parts, information, or facilities shall be strictly prohibited and invoke disciplinary action.

UNACCEPTABLE USE

Under no circumstances, a user of IT resources and facilities of the University shall be authorized to engage in any activity that is illegal under Indian or international law.

The following activities shall be prohibited in general. In case the need arises, select users can be exempted from these restrictions -

This list is, however, not exhaustive, but it provides a basic framework of activities falling into the category of unacceptable usage.

SYSTEM AND NETWORK ACTIVITIES

(a) The users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts that may harm the network's performance or security.

(b) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the university.

(c) Any infringement of copyright materials including, but not limited to, digitization and sharing of photographs from magazines, books, or other copyrighted sources/Movies/Music, and the installation of any copyrighted software for which the university or the end user does not have any active license.

(d) Accessing data, a server, an account, or any IT equipment for any purpose other than academics, research, and official work related to the university.

(e) Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws.

(f) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(g) Sharing account passwords with others or allowing the use of accounts by others including family members while working at home.

(h) Using computing assets of the University to actively engage in procuring or transmitting material that violates sexual harassment/ Human Rights or material considered hostile at the workplace.

(i) Making fraudulent offers of products, items, or services originating from any university account.

(j) Making statements about warranty, explicitly or implied, unless it is a part of normal job duties.

(k) Effecting security breaches or disruptions of network communication. Security breaches include accessing data for which the user is not an intended recipient or logging into a server or account that the user is not authorized to access unless these duties are within the scope of regular duties. For this section, disruption includes but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(l) Executing any form of network monitoring which shall intercept data not intended for the user’s host, unless this activity is a part of the user's normal job responsibility.

(m) Circumventing user authentication or security of any host, network, or account.

(n) Introducing honeypots, honeynets, or similar technology on the University network.

(o) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or the Internet/Intranet/Extranet.

EMAIL AND COMMUNICATION ACTIVITIES

While using university IT resources to access and use the Internet, the following points are to be adhered to:

1. The users must realize that they represent the University. Whenever users state an affiliation with the University, they must also indicate that "the opinions expressed are my own and not that of the university".
2. E-mail service authorized by the university shall only be used for all official correspondences after the specific notification as to the implementation of this Clause.
3. For personal correspondence, users may use the name-based e-mail ID assigned to them on the university-authorized e-mail Service.

The following activities are strictly prohibited:

1. Sending unsolicited email messages, including junk mail or other advertising material to individuals who did not specifically request such materials (email spam).
2. Any form of harassment via email, or telephone, whether through language, frequency, or size of messages.
3. Unauthorized use or forging of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the network of the University or from other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the University of Rajasthan or connected via the network of the University of Rajasthan.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Retiring or the employees being relieved and the students leaving the university shall surrender the mail ID allotted on the University of Rajasthan domain name or University of Rajasthan email server for clearing their No Dues.

BLOGGING AND SOCIAL MEDIA

In contrast to other traditional media, social media is more interactive, enables one-to-one conversation, and facilitates an instant response. However, the University is aware of the fact that on such platforms, the perception of an official and personal role and boundaries is often blurred. Therefore, while using social media for official purposes, the following may be kept in mind to smoothen interaction. Official Blogging or access to social media will be regulated by the administrator/user delegated. Limited and occasional use of the systems of the University of Rajasthan to engage in blogging is acceptable subject to the conditions specified hereinafter.

1. Social Media can be accessed only after office hours. If a user is required to use it for a part of his official assignment or collect any information during office hours, it can be permitted by the competent authority.

Exception: The following shall be exempted from the application of this rule:

(a) Users or any other official working in the role of Public Relations.

(b) Users or any other official working for community outreach under the Community Outreach Programme.

2. There shall be an absolute prohibition on the users from making any discriminatory, disparaging, defamatory, or harassing comments or bullying while blogging or using social media. The acts, omissions or any statement resulting in instigation, abatement to commit any offense, creating communal hatred, or apathy shall be strictly prohibited.
3. No user shall involve oneself in any kind of blogging resulting in compromise with the interests of the university, including its employees.
4. No user shall attribute one’s statements, opinions, or beliefs while using the university network while engaged in blogging or accessing social media.

5. Apart from following all laws of the land about peace and order as well as the handling and disclosure of copyrighted or export-controlled materials, the logos of the University of Rajasthan and any other University of Rajasthan intellectual property shall also not be used in connection with any blogging activity.

6. **Core Values for Users of Blogs and Social Media:**

   (a) **Identity:** In official communications, the user must reveal his identity and his role in the department and publish in the first person. A disclaimer may be used when appropriate.

   (b) **Authority:** Users shall not comment and respond unless authorized to do so, especially in any of the following matters:

      i. Recruitment

      ii. Examinations

      iii. Tenders

      iv. Quotations

      v. Subjudice matter

      vi. Draft Rules, Regulations, Notifications, Circulars

      vii. Injuring and damaging the reputation of any staff and the student and also the university.

   (c) **Relevance:** The users can comment on issues relevant to their area of specialization and make relevant comments without compromising the interest of the university. This will make the conversation productive and help in taking it to its logical conclusion. However, the university shall not take any responsibility for any of such comments, and it must be ensured by the user before making any comment or participating in the deliberation that the comments or ideas expressed by her/him are their ones, and not of the university.

   (d) **Professionalism:** The users must be polite, discrete, and respectful to all. They shall refrain from making any personal comments for or against any individuals or agencies. They should be careful not to politicize any kind of professional discussions.

   (e) **Compliance:** The users shall be compliant with relevant rules and regulations. They should not infringe upon IPR.

   (f) **Privacy:** Personal information about other individuals as well as one’s own private and personal details shall not be revealed unless these are meant to be made public.

DISPOSAL OF ICT EQUIPMENT

i. To ensure responsible disposal, all ICT equipment should be meticulously documented through an inventory assessment. This assessment should capture key details like manufacturer, model number, serial number, and current condition

ii. Disposal of ICT equipment must adhere to applicable laws, regulations, and environmental standards governing electronic waste management.

iii. ICT equipment deemed obsolete or no longer in use must be securely wiped of all data using approved data sanitization methods to prevent unauthorized access to sensitive information.

iv. If data wiping is not feasible due to equipment malfunction or other reasons, physical destruction of storage media (e.g., hard drives, SSDs) must be carried out to ensure data confidentiality.

v. Disposal methods such as recycling, donation, resale, or environmentally responsible disposal through certified e-waste management vendors must be considered based on the condition and usability of the ICT equipment.

vi. Disposal activities must be documented in a formal disposal log, including details of the disposed equipment, disposal method used, and relevant dates and signatures of authorized personnel involved in the disposal process.

vii. Regular reviews and audits of the disposal process must be conducted to ensure compliance with established policies, procedures, and regulatory requirements, with any identified deficiencies addressed promptly.

JURISDICTION

This policy delineates the jurisdiction for enforcement of IT policies and the responsibility of the University to adhere to government IT policies.

DISCIPLINARY AND LEGAL MEASURES

1. Deliberate breach of the provisions contained in this policy statement shall invoke disciplinary action, which may include, in addition to the penalties, denial of access to IT services and facilities offered by the university. On the other hand, if the act is covered with the meanings and definitions of offenses defined under the Indian Penal Code, 1860, Information Technology Act, 2000 (with Amendments) and any other allied laws, regulations, the legal proceedings against the person in

conflict with policy or offender shall be initiated within the prior written approval of the Competent Authority.

2. Notwithstanding the above, the Competent Authority shall have the Authority to take appropriate action in case any act is not covered under the provisions referred herein before if the act or omission affects the national interest, and interest of the university or proves otherwise offensive.

POWER TO REVISE

This IT Policy shall be subject to revision by the University from time to time.

POWER TO REMOVE THE DIFFICULTY

If any difficulty arises while implementing this policy, the competent authority can take an appropriate decision to remove the same.

BREACH OF THIS POLICY

Consequences for breaching IT policies, including enforcement measures and reporting protocols, are detailed in this policy.

REVISIONS TO POLICY

The University reserves the right to revise this policy as needed, with revisions noted in the policy's revision history. Continued use of University IT resources constitutes acceptance of revised policy terms.