POLICY FOR PROVISION OF CAMPUS-WIDE LAN SERVICES TO RESIDENTIAL QUARTERS IN RAJIV GANDHI UNIVERSITY

1. PREAMBLE

Rajiv Gandhi University, Rono Hills, Doimukh has extended its Campus wide LAN (CLAN) infrastructure to the residential quarters with a view to facilitate academic, administrative and limited personal internet access for authorized occupants. This Policy lays down the terms, conditions, regulatory framework and technical controls governing the provision and use of network services in residential quarters.

This Policy is issued in conformity with the approval of the 65th Executive Council of the university vide, and provisions of the Information Technology Act, 2000 (as amended), CERT-In Directives and notifications (as amended from time to time), guidelines/ notifications issued by the Ministry of Electronics and Information Technology (MeitY), Department of Telecommunications (DoT) and in alignment with ISO/IEC 27001 standards for information security management.

2. OBJECTIVES

The objectives of this Policy are to ensure reliable and secure network connectivity to residential quarters, to promote fair and equitable utilization of institutional bandwidth resources, to safeguard the University's IT infrastructure from misuse and cyber threats and to ensure compliance with applicable laws, standards and regulatory requirements.

3. ELIGIBILITY AND ACCOUNT CREATION

Network access shall be provided only to officially allotted residential quarters. A user account shall be created in the name of the allottee of the residential quarters. The allottee shall be solely responsible for all activities conducted using the assigned network account. Sharing of credentials beyond members of the household is prohibited and any misuse shall be attributable to the allottee.

4. SERVICE MODEL AND CHARGES

The service shall be provided under a "Residential Network Service Subscription" model. A nominal subscription fee of **₹ 150 (Rupees One Hundred Fifty only) per month shall be levied**. The said fee shall be recovered through monthly salary deduction or through such other mechanism as may be approved by the competent authority. The University reserves the right to revise the subscription fee from time to time.

5. USAGE POLICY

A maximum of three concurrent sessions or devices shall be permitted per user account at any given time. A daily data usage limit of **7 GB per account** shall be enforced. The data usage limit shall reset automatically at 00:00 hours (midnight) each day. In the event of exhaustion of the prescribed limit, the bandwidth may be throttled, or access may be temporarily restricted until the commencement of the next usage cycle. The prescribed limits are subject to revision depending upon network load and administrative considerations.

The network facility is intended primarily for academic and official purposes; however, reasonable personal use is permissible, subject to compliance with this Policy.

6. TECHNICAL ENFORCEMENT MECHANISMS

Access to the network shall be governed through a combination of technical controls including Network Access Control (NAC), captive portal-based authentication, bandwidth management systems, firewall protection and centralized monitoring mechanisms. Authentication of users shall be mandatory prior to access. Device registration and MAC address binding may be enforced as deemed necessary.

A centralized captive portal shall be deployed for user authentication, session management and enforcement of usage limits. The University shall maintain logs pertaining to user activity, including IP allocation, session details and other metadata as required under applicable laws. Such logs shall be retained for a minimum period as prescribed under CERT-In Directions or any other applicable regulations.

Content filtering and firewall systems shall be implemented to restrict access to malicious, unlawful, or prohibited content in accordance with Government directives.

7. ACCEPTABLE USE POLICY (AUP)

Users shall use the network in compliance with all applicable laws of India and in a responsible and ethical manner. Activities that adversely impact network performance or compromise security shall not be permitted. Accessing, transmitting, or storing unlawful, obscene, or copyrighted content without authorization is prohibited. Any attempt to engage in hacking, phishing, spoofing, running unauthorized servers, VPNs, proxy services, or undertaking commercial activities without prior approval shall constitute a violation of this Policy.

8. SECURITY, MONITORING AND SUPPORT

The Computer Centre shall have the authority to monitor network usage for ensuring security, regulatory compliance and performance optimization. Users shall ensure that their devices are adequately secured with updated antivirus software and system patches and that login credentials are not shared.

Any security incident or suspected compromise shall be reported immediately to the Computer Centre. For any technical assistance or support related to the network services, users may contact the Computer Centre through the officially notified communication channels.

9. PRIVACY

While reasonable efforts shall be made to respect user privacy, monitoring may be undertaken for legitimate purposes including network security, legal compliance, and investigation of incidents, in accordance with applicable laws. University will share user access logs with competent law enforcement agencies as and when sought for.

10. SERVICE LEVEL AND LIMITATIONS

The network service shall be provided on a best-effort basis. The University does not guarantee uninterrupted or error-free service. Interruptions may occur due to maintenance activities, network upgrades, power failures, or issues attributable to external service providers.

11. VIOLATIONS AND PENALTIES

Any violation of this Policy may result in warning, temporary suspension, permanent disconnection, or disciplinary action as per university rules.

12. TERMINATION OF SERVICE

Network access shall stand terminated upon vacation of the residential quarter by the allottee, discontinuation of the service, or upon violation of this Policy. Any outstanding dues shall be settled prior to termination.

13. LIABILITY

The University shall not be liable for any loss of data, security breaches at the user end, or misuse of credentials by the user or members of the household.

14. AUDIT AND COMPLIANCE

The system and associated processes shall be subject to periodic audit to ensure compliance with ISO/IEC 27001 standards and directives issued by CERT-In and MeitY. Necessary documentation, logs and records shall be maintained for audit and review purposes. Periodic risk assessments and security reviews shall be conducted.

15. AMENDMENTS

The University reserves the right to amend, modify, revise, review, or update any provision of this Policy, including the subscription fee and other related charges, from time to time, as may be considered necessary in view of administrative exigencies, operational requirements, maintenance and upgradation of services, financial implications, or any other institutional considerations.

The subscription fee may accordingly be reviewed and revised periodically by the University, as deemed appropriate. All such amendments, revisions, modifications or updates shall be notified through the official communication channels of the University and shall come into force with effect from the date of issuance of such notification, whereupon the same shall be binding on all concerned.

16. GOVERNING LAW

This Policy shall be governed by the laws of India, including but not limited to the Information Technology Act, 2000, CERT-In Directions and guidelines issued by DoT and MeitY.

17. MANDATORY APPLICABILITY AND DEEMED ACCEPTANCE

The provisions of this Policy shall apply mandatorily to all residential quarters where network services are provisioned. The allottee of the residential quarter shall be deemed to have accepted and shall remain bound by this Policy upon activation, assignment, or use of the network service, irrespective of whether any separate subscription request has been submitted.