



National Institute of Technology Silchar

Central Computer Center (CCC)

Institute Internet Usage Policy

This document outlines the governance of the Internet usage within the Institute, ensuring efficient, transparent, and ethical use of the network resources provided to faculty, staff, students, and other stakeholders.

1. NETWORK CONFIGURATION

Link Aggregation: Utilize link aggregation to combine multiple Internet Service Provider (ISP) connections to enhance fault tolerance and increase bandwidth throughput beyond that provided by a single ISP.

User-wise ISP Preference: Assign ISP preferences based on user roles and departmental requirements to optimize bandwidth utilization and cost-efficiency.

2. BANDWIDTH MANAGEMENT

General Bandwidth Usage: Each user is allocated 5 GB of data per day at full bandwidth. Post this limit, the speed may be reduced to ensure fair usage.

Priority Settings: Virtual conferencing shall receive higher priority in bandwidth allocation to ensure smooth communication for critical meetings and collaborations.

Dedicated Links for Key Positions: The Director and Registrar shall have dedicated, prioritized Internet links to ensure uninterrupted service for administrative functions.

3. TRANSPARENCY AND MONITORING

Utilization Reports: Network utilization will be monitored and reported through graphical statistics to provide transparency and facilitate better decision-making regarding network planning and performance optimization.

Captive Portal: Implement a captive portal for user authentication which helps in identifying and managing the network usage on a per-user basis.

4. POLICY ON LOGS AND REPORTING

Log sharing will be governed by strict protocols to protect user privacy and institutional integrity:

Vigilance Issues: Logs can be shared internally for investigation of vigilance issues upon approval by the Director, NIT Silchar.

ISP Issues: For issues raised by ISPs, logs will be shared in compliance with legal requirements and institutional policies.

Unethical Communication: In cases of detection of unethical communication, logs can be reviewed by the approval from the Director, NIT Silchar.



National Institute of Technology Silchar

Central Computer Center (CCC)

General Access to Logs: Access to logs for any other reasons must be approved by the Director, NIT Silchar.

5. CONTENT FILTERING AND BLOCKING POLICY

Block Categories for Students: To ensure a safe and productive educational environment, the following categories of websites and content will be blocked:

1. Alcohol & Tobacco
2. Criminal Activity
3. Gambling
4. Hacking
5. Nudity and Adult Content
6. Peer-to-peer & Torrents
7. Sex Education (unless approved for academic purposes)
8. Sexually Explicit Material
9. Spam URLs
10. Suspicious Sites
11. Weapons

6. IMPLEMENTATION AND COMPLIANCE

Captive Portal Usage: All users must authenticate through the captive portal to access the Internet, helping in monitoring and managing individual usage.

Policy Enforcement: Non-compliance with the above policies may result in disciplinary action, including but not limited to temporary or permanent revocation of network access privileges.

7. AMENDMENTS AND REVISIONS

This policy is subject to revisions and amendments at any time to adapt to technological advancements, changes in legal requirements, or institutional priorities.