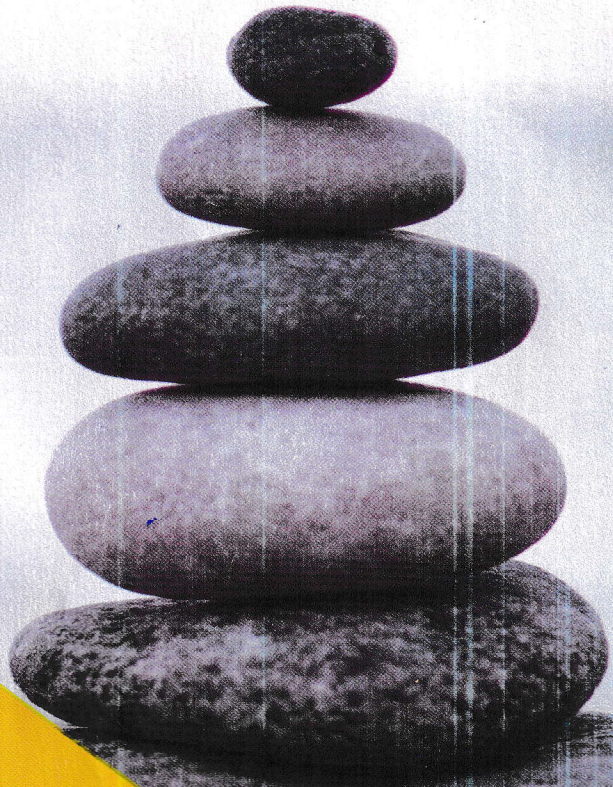


# Network Policy

Version 1.0\*



**University of North Bengal**  
Computer Center

## Policy Focus

### PURPOSE

To define the University network and establish operational provisions governing use and operation of the network.

### APPLIES TO

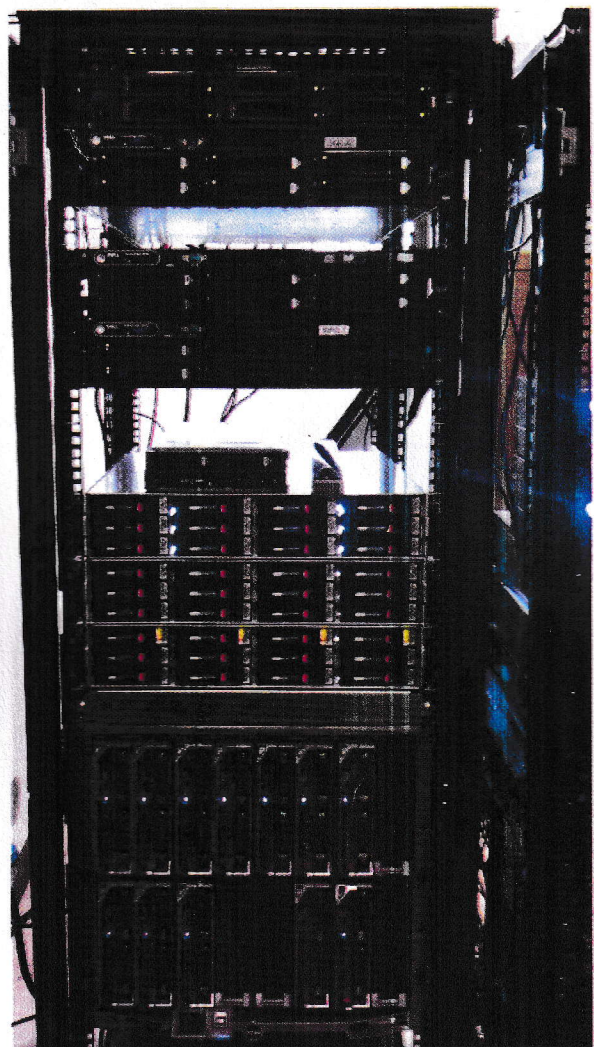
This policy applies to all users directly or virtually connected to the University network.

### CAMPUS

Raja Rammohunpur Campus located at Raja Rammohunpur, District-Darjeeling, PIN-734013, West Bengal, India

### CONSEQUENCES

Any individual who violates this policy may lose computer or network access privileges and may be subject to disciplinary action in accordance with and subject to appropriate University policy and procedures





## PRINCIPLES

The University Network is an infrastructure of electronic and optical distribution hardware, control software, and wired and wireless media. The University network utilizes various technologies to transport data. The University network begins at the point where an end-user device gains access to this infrastructure and ends at the point where the University network attaches to external non-NBU networks.

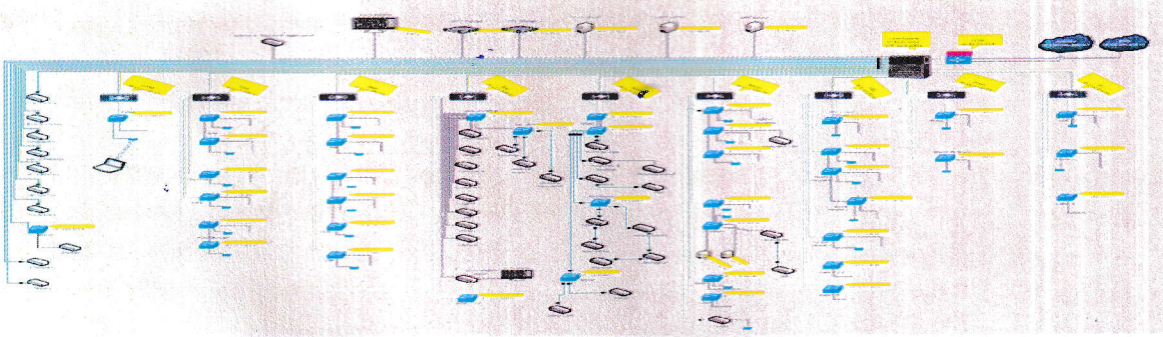
End-user devices that indirectly connect via a third-party telecommunications provider (a connection made to the NBU network via a home broadband or dial up connection for example) are not considered part of the University network.

The University will adopt a uniform set of standards, installation practices, processes, procedures, and operational criteria in the construction, use, and ongoing management of the University network to ensure its secure, effective and efficient use.

The priorities for the University network are safety, security, economy, reliability, and capability. The University's goal is to ensure the integrity and stability of the University network, as well as the efficiency and effectiveness of its construction and operation.

Providing a centrally managed enterprise class institution wide network is most effective and efficient method for achieving University's goals in information transport. This reduces the total cost of ownership to the University and promotes the availability and reliability of its information transport systems for all users. Through central planning and management, the University ensures that the network infrastructure is constructed and operated in an integrated, effective, and efficient manner.

The University network is for the use of the University as a whole and is managed for the benefit of all University users. Therefore, the network is designed and implemented to handle a wide variety of information transport requirements. This network is designed to satisfy most user needs for the transport of information.



## GENERAL POLICY PROVISIONS

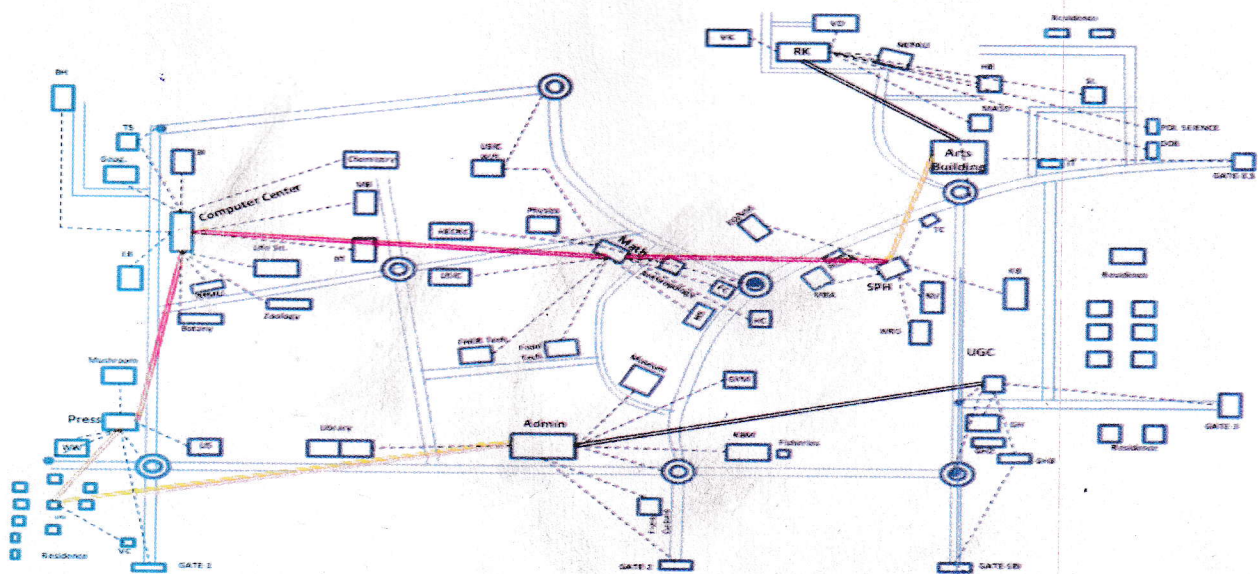
- Information Technology will manage and administer the University network through its Computer Centre.
- Use of the University network will depend on the availability of network bandwidth, usage of electronic resources and count of simultaneous access and will be administered by Computer Centre, NBU.
- All physical connections to the University network must be made in accordance with the industry best practices and standards.
- All wireless connections to the University network must be made in accordance with, NBU's [wireless policy](#). (Refer Annexure)
- All devices connecting to the University network must be registered (in stock) either centrally or at department level.
- The configuration and operation of devices connecting to the University network must comply with all applicable University security policies, procedures, and practices.
- The Computer Centre will determine the security specifications and standards for devices connected to the University data network.
- All devices/users connecting to the University data network through NBU's Virtual Private Network (VPN) must use the centrally-provided service only and comply with NBU's [SSL VPN Connectivity mechanism](#). (Refer Annexure)
- Computer Centre will determine the technical specifications, installation practices, standards, and operational criteria for the management and operation of the University network.

- The University data network shall utilize the open standard suite of protocols collectively known as the Internet Protocol (IP). Vendor proprietary protocols will not be routed over the University data network.
- Departments/users may not attempt to implement their own network infrastructure or extend the University network without permission from Computer Centre. This includes, but is not limited to, basic network devices such as repeaters, switches, routers, network firewalls, wireless access points, or virtual extensions using tunneling technologies such as Virtual Private Networking (VPN) hardware and/or software. Units/users may not offer alternative methods of access to the University network, such as modems.
- All the University Departments, except for few with very less number of administrative users, will be allocated separate partitioned and isolated broadcast domain or VLAN.
- All the primary switches at the threshold of each VLAN will be managed directly from Computer Centre.
- Devices connecting to the University's data network must use the central Dynamic Host Control Protocol server for authorization to use the University Network.
- All individual users should use their own authentication token to use the University Network either on LAN or on wireless or through VPN. Any registered students of the University pursuing graduation or post-graduation are eligible to get these credentials from Computer Centre on completion of admission related process. Any research students and faculty or administrative employees have to apply for these credentials through the "Campus Connect" app on NBU official website, and for them an email account at nbu.ac.in is a prerequisite.
- The University recognizes that certain organizations/departments may require their own information transport networks for academic, research, or other special purposes. Any such information transport need must be coordinated through NBU Computer Centre.
- Any addition/alteration of physical network connection will be prioritized based on nature, urgency, size of request queue and availability of required resources.
- **The Head, Computer Centre can make exceptions to the provisions of this policy in accordance with overall network management and reliability requirements and user needs.**



## Responsibility of Computer Centre

- Monitoring rules, regulations, guidelines, best practices and standards suggested by Government agencies.
- Monitoring the performance of the University network and ensuring its reliability. Computer Centre to build/procure a NMS software to monitor the University Network proactively.
- Ensuring compliance with the University's privacy practices in relation to network functions in consultation with the University authority.
- Providing systems to ensure user registration and the purging of unregistered users.
- Providing mechanism for communicating network health and planned maintenance downtime to users.
- Provide user training based on need, either on one-to-one basis or as a group.
- Any grievance or complaint related to University Network to be responded in 4 hours on business days starting from time it got received at [cchelpdesk@nbu.ac.in](mailto:cchelpdesk@nbu.ac.in) inbox based on its priority, severity and size of impacted population.
- Computer Centre will maintain a log book for all the requests received associated to University Network, for proper monitoring.



## Responsibility of Departments / Users

- For new service, requesting changes to existing service, and/or reporting maintenance issues of University Network mail needs to be sent to [cchelpdesk@nbu.ac.in](mailto:cchelpdesk@nbu.ac.in) or hard-copy application to be shares with Head, Computer Centre. No other way of communication of grievance or complaint will be monitored by Computer Centre.
- Any addition/alteration of physical network connection should be routed through departmental Head only to Head, Computer Center.
- Departments will be responsible for expenses associated with correction of any unauthorized installation, modification, or resulting repair.
- Department will be responsible for data loss or network security compromise in their respective VLAN due unauthorized attempt to implement their own network infrastructure or extend the University network without permission from Computer Centre.



**CONTACT:**

System Manager & Head, Computer Centre  
University of North Bengal  
[systemmanager@nbu.ac.in](mailto:systemmanager@nbu.ac.in)

**APPROVED BY:**

Vice-Chancellor, University of North Bengal

**APPROVED ON:**

Friday, May 10, 2019

**EFFECTIVE ON:**

Friday, May 10, 2019

**REVIEW CYCLE:**

Annual or as Needed

**University of North Bengal**

Raja Rammohunpur, P.O. - NBU, District  
Darjeeling, PIN - 734013, West Bengal, India

[www.nbu.ac.in](http://www.nbu.ac.in)