Network Access and Monitoring Policy

The network must be designed and configured to deliver levels of performance, security and reliability suitable for the college's needs, whilst providing a high degree of control over access. Users of college networks are to be explicitly advised that normal operational network management procedures will include: probing devices to test their security and the monitoring of network traffic to detect operational problems or possible policy violations.

Connecting devices to the network

Ownership of networked devices: Only devices owned by the college may be connected to the "wired" network. Privately owned devices may only be connected to the "wired" network in special circumstances approved by the Head of Department. Privately or college owned laptops/PCs may be connected to the wireless network. All devices whether privately owned, or owned by other organisations, must meet the hardware and software requirements, and their usage must conform to college policies.

Administration of networked devices

Every networked device must be associated with an identifiable and contactable person responsible for its administration. Devices for which the administrator cannot be identified or contacted are liable to be removed from the network.

DHCP Servers

The Computer Centre provides DHCP service in all VLANs of the college to enable automatic IP configuration of clients. Installation of unauthorized DHCP servers, without explicit consent from the Centre, will not be not permitted in any Sreenidhi VLAN as such DHCP servers can interfere with normal usage.

Wi-Fi routers and Access Points (APs)

Installation of unprotected Wi-Fi routers

Installation of Wi-Fi routers in the college campus will not be permitted without explicit consent from the Computer Centre. All users should use the authorized WI FI SSIDs for Wi-Fi access and verify the authenticity of the Wi-Fi routers

All Wi-Fi routers should have at least WPA2-PSK (pre-shared key with WPA2 encryption) standard security enabled.

The GOI regulation prohibits shared access of Wi-Fi resources and mandates Wi-Fi access only through a central authentication mechanism. In view of this, 802.1x (WPA2-Enterprise) is the minimum acceptable standard for setting up Wi-Fi access

Connecting other ISP networks to Sreenidhi LAN

It is strictly prohibited to connect other ISP networks (not obtained through the Computer Centre) to the Sreenidhi Network.

In case it is allowed for research or special operational needs it will be the responsibility of the facility in-charge to completely firewall the external network from the Sreenidhi Network both for inward and outward connections.

Virtual Private Network (VPN) and Secure Shell (SSH) Access

It is strictly prohibited to setup unauthorized VPN or SSH access facilities for connecting to Sreenidhi Network from outside without explicit consent from the Computer Centre. The VPN facility, if made available at the Computer Centre, should be used for such purposes.

It is also prohibited to facilitate external access to the Sreenidhi network using any terminal sharing or other similar software. The VPN facility shall be made available to needy faculty, staff and research scholars on the recommendation of their Head/Supervisor.

Access Monitoring

ARP monitoring is to be enabled on all VLANs and all IP address to MAC address mappings will be logged and maintained for a period of three months.

Network Usage Monitoring

Usage of Sreenidhi Network (wired `& wireless) will be monitored on daily/weekly schedule and access usage may incur financial penalties or suspension of privileges.

Residents of Faculty/Staff/Officers on the campus and Sreenidhi Guests shall be provided access to network (wired or wireless) and internet.

Internet access (wired LAN)

Internet access from the wired LAN will be available and access will be restricted to ftp, http and https protocols through designated ports. All accesses will be logged along with the URL, time of access and uid of the user. The logs will be maintained for a period of three months.

In addition, for specified network ports 802.1X authenticated LAN services may be provided on request where technically feasible. In these authenticated ports, all ports can be opened on request.

Internet access (wireless LAN)

Connecting to the SSIDs will require 802.1x authentication and all wireless network traffic will be encrypted using WPA/WPA2 standards. All authentications will be logged along with time of access, uid of the user, registered DHCP IP address and the MAC address of the accessing device.

All logs will be maintained for a period of minimum three months.

Static IP addresses for inward connections

On special requests static external IP addresses may be allocated to specific servers for access from outside on specific ports. This may be required for designated web servers and other research facilities. In all such cases it will be the responsibility of the facility in-charge to install proper firewall and security measures to ensure that the access is restricted to the specific server and the Sreenidhi network is completely protected from external accesses.

Unrestricted external access from designated servers

Unrestricted access to internet access may be given from specific servers on request for special research and operational needs. It will be the responsibility of the facility in-charges to ensure that access to such a facility is restricted and the users adhere to the relevant policies of the college.

Access logs are maintained for accesses on all ports as required by GOI regulations