Network access and monitoring policy

IIT Delhi is required by the IT Act 2009 and the GOI guidelines to be able to associate every internet access using its facilities to specific users and maintain logs of all such accesses for a minimum period of three months. Please see, for instance, Wifi access guidelines and liability of network service providers
(clauses 33 and 34).

In view of the above, and also keeping in mind the internal security requirement of IITD, the **Deans Committee**
in its meeting on December 16, 2016, has decided on the following
network access and monitoring policy
.

DHCP servers

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

Wifi routers and access points

1. Installation of unprotected WiFi routers is banned by a GOI regulation .
2. Installation of Wifi routers in the academic area will not be permitted without explicit consent from CSC. All users should use the authorized IITD_WIFI SSIDs for Wifi access and verify the authencity of the WiFi routers using the digital certificate duly signed by the IITD CA
or a globally valid CA..

3. All WiFi routers that provide connection to the IITD LAN should have at least WPA2-PSK (pre-shared key with WPA2 encryption) standard security enabled. This should be sufficient **for individual use and residences.**

4. The GOI regulation prohibits shared access of WiFi resources and mandates WiFi

access only through a central authentication mechanism. In view of this, 802.1x (WPA2-Enterprise) is the minimum acceptable standard for setting up WifI access in the **academic area**

.

Connecting other ISP networks to IITD LAN

It is strictly prohibited to connect other ISP networks (not obtained thorugh CSC) to the IITD LAN without explicit consent from CSC. In case it is allowed due to research or operational needs it will be the responsibility of the facility in-charge to completely firewall the external network from the IITD VLAN, both for inward and outward connections.

VPN and ssh access to IITD LAN

It is strictly prohibited to setup unauthorized VPN or ssh access facilities for connecting to IITD LAN from outside without explicit consent from CSC. The VPN facility available at CSC should be used for such purposes. It is also prohibited to facilitate external access to the IITD network using any terminal sharing or other similar software. The VPN facility is currently available to faculty, staff and part-time phd/ part-time ms(R) students on the recommendation of their supervisor.

Access monitoring in IITD VLANs

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 in IITD

Usage of IIT Delhis' network (wired & wireless) will be monitored on daily/weekly secdule and access usage may incur financial panelties or suspension of privileges.

Internet access from academic area (wired LAN)

Internet access from the wired LAN in the academic area will only be available through the designated proxy servers and no NAT/PAT will be enabled. Access through the proxy servers will be restricted to ftp, http and https protocols (ports 21, 80, 443, 8080 and 8443). 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 from academic area (wireless LAN)

Connecting to the SSIDs *IITD_WIFI*, *IITD_Secure_GUEST*, and *eduroam* 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.

Since connections to IITD WiFi are authenticated, access to services on all other safe ports (except port 25) will be open and made available through NAT/PAT at the IITD firewall. VPN connectivity for popular protocols will also be enabled at the firewall where logs will be maintained. The logs will include the time of access and the NAT/PAT mappings. (**Because of a large number of indiscriminate bittorrent downloads of copyrighted material, and the subsequent legal notices that IITD received, this facility has been withdrawn from August 8, 2014. Restored only for faculty from November 17, 2014. Restored for staff & visiting researchers from Sep 16, 2016. It will be restored for all users soon. They will need to accept the updated IITD IT policies**).

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

Internet access from the Wifi SSID *IITD_GUEST/IITD_Guests*

The SSID IITD_GUEST/IITD_Guests is being phased out and replaced with IITD_Secure_GUEST which is 802.1x authenticated and allows a much larger set of open ports including outside access to ssh and vpn.

The Wifi SSID IITD_GUEST/IIT*D_Guests is* available throughout the academic area, the Guest houses and Hostels. This Wifi access will be unsecured without any encryption of network traffic (except for accessing https pages). Accessing the network using this SSID will require

authentication at a IITD proxy captive portal available on https to which a guest will automatically be redirected. Only short term visitors to IITD will be allowed to login through this captive portal.

After successful login at the captive portal, all accesses to internet will be routed through a transparent proxy server where all accesses will be logged for a period of at least three months. Access to internet services will restricted to http, and https. However, no access to the IITD internal LAN will be allowed from this Wifi SSID except to IITD webservers. All accesses will be logged along with the authenticated uid.

It will be responsibility of the account creator to verify the identity of the guest and record the mobile phone number of the guest, as per GOI guidelines, at the time of creating guest accounts. CSC will set up a facility to communicate the password to the guest through SMS on the recorded mobile phone.

Internet access from Guest Houses

All accesses using wired LAN will have a policy identical to the intenet access policy using the wired LAN from the academic area. All access using Wifi SSIDs *IITD_WIFI* will have a policy identical to the internet access policy through IITD Wifi.

All accesses using WiFi SSID *IITD_GUEST* & IITD_Secure_GUEST will be as descibed above.

Internet access from the hostels

Internet access from the hostels will only be available through the designated proxy servers and no NAT/PAT will be enabled. Access through the proxy servers will be restricted to ftp, http and https protocols (ports 21, 80, 443, 8080 and 8443). 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 WiFi service in Hostel Common Areas is provided. This operates throughout the day and night and the policies will be as applicable in the academic area as far as Wifi Access is concerned.

Internet access from faculty homes (GPON/ADSL)

All faculty members and other members of staff who have been provided with GPON or ADSL

facility at their residences will be provided with fixed IP addresses for connecting to the IITD LAN. The mapping of the IP addresses to internal telephone numbers will be maintained by the telephone department and made available to CSC in the case of ADSL. The CSC shall maintain the mapping in case of GPON.

Internet access will be available through NAT/PAT at the firewall. All external accesses will be logged at the firewall which will include the time of access and the NAT/PAT mappings.

Peer-to-peer and UDP connections is blocked for the ADSL network. Also, TCP services on port 25 will be blocked. For GPON all ports other than 25 are open.

Internet access from TBIU

Each TBIU unit will be provided with only one network socket point connected to a IITD backbone switch. Only one fixed IP address will be allowed from each socket and the TBIU units will be expected set up their own router with NAT/PAT to allow other machines in their premises to connect through the single network point. The internet access will be unrestricted. All internet accesses will be the sole responsibility of the TBIU units and they should follow all GOI guidelines.

FITT will coordinate with CSC to assign one IP address per TBIU and to make them aware of this policy,

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 IITD network is completely protected from external accesses. No shell or VPN access should be provided without explicit consent of CSC.

Unsrestricted external access from designated servers

Unrestricted access to internet access bypassing the proxy servers may be given from specific servers on request for special research and operational needs. It will be the responsibilty of the facility in-charges to ensure that

1. access to such a facility is restricted and users do not use such a facility to access the internet bypassing the proxy servers
2. IITD IT usage policy and privacy policy are strictly adhered to.
3. Access logs are maintained for accesses on all ports as required by GOI regulations.