Last Updated on 23-Sep2014

IIITD Internet Usage and Privacy Policy

All IIIT Delhi users are required to know, understand and abide by the usage policy for Internet access through the institute network. These policies are formulated as a requirement of the IT Act 2010 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. These policies also help in providing secure and stable Internet access to IIITD users and protect their privacy. Major relevant policies are:

1. IP Address Assignment

IIITD provides DHCP service in all VLANs to enable automatic IP configuration of clients based on their MAC address. MAC addresses of all the desktops, laptops and mobile devices to be used in academic area (academic block, library and service block) and student hostels (boys hostel, girls hostel and dining block) need to be registered with the IT Department.

Usage of static IPs and installation of unauthorized DHCP servers, without explicit consent from the IT Department, will not be not permitted in any IIITD VLAN, as it can interfere with normal usage.

2. Internet Access through Wired and Wireless LANin Academic Area and Student Hostels

IIITD provides wired LAN and secure Wi-Fi access in academic area and student hostels.Any user can access Internet by using wired or wireless Internet connection but it is mandatory to login to his/her own firewall account to get access to Internet.

Wi-Fi connectivity is provided through *Faculty-Staff*, *Sensor*, *Students* and*Eduroam* SSIDs. The Wi-Fi access is protected through PSK (Pre-Shared Key) in the wireless media and further through firewall login for Internet access. IT Department is also planning to implement WPA2 for better security.

Since connections to Internet are authenticated, access to services on all ports is open and made available through NAT at the IIITD firewall. VPN connectivity for popular protocols is also enabled at the firewall. The logs of Internet access are maintained by the IT Department. The logs include the username, time of access, destination URL, destination port and the NAT mappings. All logs are maintained for a period of three months.

There is no restriction on bandwidth except in student hostels where the overall bandwidth allocated for wired LAN connectivity is currently 30 Mbps. The restriction may be reviewed based on requirements.

Installation of Wi-Fi routers in the academic area and student hostels is notpermitted without explicit consent from IT Department. All users should use the authorized IIITD Wi-Fi SSIDs for Wi-Fi Access.

It is strictly prohibited to connect other ISP networks to the IIITD LAN without explicit consent from IT Department. In case it is allowed due to research or operational needs, it will be the responsibility of the faculty in-charge to completely firewall the external network from the IIITD VLAN, both for inward and outward connections.

3. Internet Access from Faculty Housing Block

All faculty residences have been provided wired LAN facility only at their residences. They can install their personal wireless router and access Internet services by following the following procedure:

1. All IP address allocated through DHCP to any machine/wireless router in the residence block will be based on the MAC address.
2. If a user is using a Wireless Router, they can register the MAC address of the router with the IT Department. No wireless device (laptop, mobile, tab etc.) behind the router needs to be registered.
3. If a user has a wireless router, but it has been specifically configured in bridge mode, they can register the MAC address of all the devices (wired and wireless) with the IT Department.
4. If a user has a machine which is directly connected to the LAN port (desktops or laptops connected to the LAN port) they can register the MAC address of the device with the IT Department.
5. For all the devices which are behind a wireless router (including guest devices) or a device connected to LAN but has its MAC registered, firewall login will be bypassed. For other devices (unregistered user/guest devices connected to LAN or bridged AP), firewall login will be enabled.

6. For the residence machine(s) which are not bypassed through firewall login, users can use their existing firewall login-password. However if they need a separate login, they can apply for the same by sending a mail to the IT Department.
7. All mails for the IT team can be sent to helpdesk@iiitd.ac.in. IT Department can also help in identifying whether a Wireless Router is being used in the residence or not and what are the MAC addresses of various devices which need to be registered.

4. Guest Internet Access

The Wi-Fi SSID *Guest* is available throughout the academic area and the Guest houses. This Wi-Fi access is secured using PSK forwireless network traffic and also has a firewall username and password which is changed every fortnight by the IT Department. This username and password are shared on specific requests from the visitors. Only short term visitors to IIITD will be allowed to login through this captive portal. For using Guest SSID Mac Address registration is not required.

After successful login at the captive portal, all accesses to Internet are routed through the firewall where all accesses are logged for a period of at least three months.

It is the responsibility of the IT Department to record the identity of the guest, as per GOI guidelines, at the time of sharing credentials.

5. VPN and SSH access to IIITD LAN

It is strictly prohibited to setup unauthorized VPN or ssh access facilities for connecting to IIITD LAN from outside without explicit consent from IIITD. The VPN facility available at IT Department (currently only to faculty and some research scholars) should be used for such purposes. It is also prohibited to facilitate external access to the IIITD network using any terminal sharing or other similar software except for project and research purposes. SSH primarily should be done through SSH gateway server only.

6. Static Public 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, approval form IT committee is required. It will be the responsibility of the facility in-charge to ensure that the access is restricted to the specific server and the IIITD network is completely protected from external accesses. No shell or VPN access should be provided without explicit consent of IT committee.

7. Unrestricted External Access from Designated Servers

Unrestricted access to Internet access bypassing the firewall login 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:

1. Access to such a facility is restricted and users do not use such a facility to access the Internet for unlawful activities.
2. IIITD IT usage and privacy policy are strictly adhered to.
3. Access logs are maintained at servers and firewall level for accesses on all ports as required by GOI regulations.

8. Internet Content Filtering Rules

The current Internet content filtering rules applicable to various categories of users is available here. These rules may be modified from time to time based on requirements and changes in usage policies. Any request for temporary/permanent relaxation on filtering rules will have to be approved by the IT committee.

9. Internet Access Monitoring and Access Log View

The logs of complete Internet activity are maintained in a syslog server and firewall. The IT Department may monitor the Internet activity or view the Internet access logs in case of following circumstances:

1. Excessive utilization of Internet bandwidth has been detected.
2. There is s security breach which needs to be traced and analyzed.
3. Malicious traffic from some machine(s) has been detected.
4. There is a complaint from Law Enforcement Agencies.

In the scenarios 1-3 above, Internet access logs from firewall can be viewed as and when required by IT Department after approval of the IT committee to identify the source or cause of the issue. In scenario 4, Internet access logs from firewall can be viewed by IT Department only on prior approval from Director and IT committee.

Access to syslog server and firewall logs will be available only to Senior System Manager and Assistant Manager of IT Department and will be protected through best practices for server access security.

10. Action Against Misuse

If any user is found to be misusing the Internet facilities by the way of downloading of restricted or copyrighted content, security breach, hacking passwords of other users, sending inappropriate mails or any other activity which can be categorized as unethical, the case will be referred to the Director, Dean of Academic Affairs or Registrar, as applicable.

★ Note :- On 23/09/2014, Firewall web filter Categories updated.