1. For visitors who may be visiting IITD **for more than 7 days**, and for contract employees, all faculty members and designated staff from the departments/centers can directly create user accounts from https://userm.iitd.ac.in/usermanage/create-account.html . After account creation, the hard copy of the account creation details will have to be sent to the CSC for validation, without which the account will get automatically deactivated after 7 days. These accounts will have email and disk space facilities.

2. For Guests/Workshops and other short term visitors who may be visiting IITD **for less than 7 days** , their faculty hosts can directly create internet access accounts. These accounts will not have IITD email and disk space facilities, but the procedure for WiFi and internet accesses will be simpler. The faculty host must create an account for the guest at https://www.cc.iitd.ac.in/usermanage/guest-account.html and note down the randomly generated password. The account will be automatically deleted after the specified expiry date.

There are two possible methods the guest can use the Internet:

- Method 1:

1.
1. The guest will connect to "IITD_Secure_GUEST" WiFi in Academic & Guest Houses area and provide his user and password.
2. No proxy or other restrictions will apply for this connection. Guest must abide by all IITD IT Polcies.

- Method 2:

1. The guest will connect to "IITD_Guests" (Being Repkaced by "IITD_GUEST") WiFi in hostel area or "IITD_GUEST" WiFi in academic area.
2. The guest will disable all the proxy options in the browser.

3. The guest will be redirected to a secure https authentication page automatically when she/he starts browsing the first non-https site.

4. The https page will present the guest with a certificate. The guest should verify the authenticity of the certificate/server by verifying the following signatures:

- SHA1 Fingerprint=F3 C9 5B 7A 96 0E 54 6A 5B F2 85 42 EE 12 D4 FF D4 8E D2 72
- MD5 Fingerprint=CC 49 1F A2 31 52 69 74 E2 AA 64 AB BE D0 5D 42

or

- SHA1 Fingerprint=37 CB 24 EB 54 59 57 27 AA 48 D6 EE 25 02 91 39 1B E1 09 B7
- MD5 Fingerprint=10 96 2F A3 FB 57 F3 AB 3D 3B 52 E4 05 38 D3 4F

- After verifying the certificate, the guest will be presented with an authentication page. After successful authentication, the guest will need to keep the authentication window open and can browse from another window (CTRL-N) or tab (CTRL-T).