University of Delhi Remote Access Facility
Policy Guidelines

Purpose

This procedure must be followed to ensure the integrity of the University's network and to protect all users of University systems.

Systems for connecting remote users to a network often provide the user with many of the same privileges as those connected directly to the network. This requires that the remote computer must adhere to University of Delhi Information Technology Policies, Procedures and Guidelines, and be managed in a way that is compatible with standards maintained by other networked computers.

Remote Access Policy

1. The Remote Access facility to electronic resources is available only to the authorized users of the University i.e. Faculty Members, Researchers, Students and Staff of University of Delhi.

2. Remote access to the University network is available through the University VPN service and Commercial Software subscribed by the University.

3. The University VPN service is managed and operated by DUCC as part of the overall University network infrastructure.

4. Access to the University VPN service shall be via authenticated login utilizing the University Authentication System.

5. An individual having DU domain name email ID and Password is automatically entitled to login VPN system.

6. Remote access through commercial platform shall be provided on verification of credentials.

7. Users of the University VPN service are bound by DUCC Regulation and Policies.

8. The VPN service is considered an extension of the University Network. As such, systems being used from off-campus locations to connect to the VPN service shall be

considered part of the University Network. University of Delhi Computer Regulations and Policies shall therefore apply.

9. Use of the VPN service should only occur from trusted computer systems. This excludes Internet cafes and other such public access computers.

10. It is the responsibility of remote users to ensure that reasonable measures have been taken to secure the Remote Host used to access University of Delhi Electronic Resources. This standard applies to all remote users of University of Delhi.

11. It is the responsibility of Remote Users to take reasonable precautions to ensure their remote access connections are secured from interception, eavesdropping, or misuse.

12. The remote users must not allow other users to access University devices or systems with their account, nor allow other uses to route traffic through their VPN connection.

13. Remote access from public workstations, Web cafes, kiosks, etc. should be avoided as such public machines are not secure and may result in login credentials being compromised.

14. The remote user should ensure that computers must be running antivirus software that is automatically updated on a daily basis. Computers must be updated with the latest operating system security patches and be set to automatically update the operating system on a regular basis.

15. Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.