



UPSDC- VPN SERVICE REQUEST FORM V2.0

1	Requester Name	
2	Organization Name / Department	
3	Designation	
4	Mail-id (@gov.in/@nic.in/@ac.in)	
5	Mobile No.	
6	Postal Address	
7	Purpose of VPN Service	
8	Permission for VPN	-VPN User Name: -Destination IP Address: -Port No.:
9	Requested Services	
10	Request Date	

Requester

Departmental Head

(Signature & Stamp)

(Signature & Stamp)

Nodal Officer, UPSDC

(Signature & Stamp)



Virtual Private Network User Policy

Purpose

The purpose of this policy is to provide guidelines for connecting internal servers hosted in UPSDC to minimize potential exposure of unauthorized users and remote Access of internal Servers from Internet over IPSec or SSL.

Scope

This policy applies to authorized users of government departments of UP intending to access internal servers or applications hosted in UPSDC for remote administration, Site and database updating or secure access to Intranet applications.

Policy

Introduction

A virtual private network (VPN) has being traditionally used to connect remote users and internal servers hosted in UPSDC over Internet to access sensitive data. VPN creates a virtual “tunnel” connecting two endpoints by encrypting end to end communication and protecting the data from unauthorized access or interception. Departmental users, who require seamless access to Internal Server for regular work, can use IPSec VPN or Client based SSL VPN from any Internet Service Provider and access internal departmental applications & databases, do remote administration, monitoring and management of resources which are otherwise not accessible from Internet.

VPN access will only be provided to servers hosted in UPSDC and behind firewall. All forms, procedures and documents related to VPN can be collected from UPDESCO. UPDESCO will not be responsible of any activities done in the application / DB even if the connection is established through remote VPN. Department should take necessary precaution to secure their application/DB.

VPN User Request

- VPN connection user is provided to authorize officers from state govt. departments/statutory bodies.
- VPN user can be created for Additional Chief Secretary/ Principal Secretary/ Special Secretary /Head of Department/ Director/ Joint Director or their Government Officer.
- The Verification of the users shall be done by the authorized representative from the concerned department
- VPN user from respective department has to fill the request form, and get it signed by Additional Chief Secretary/ Principal Secretary/ Special Secretary /Head of Department/ Director/ Joint Director.
- Signed VPN request form has to submit to UPDESCO for further approval.

VPN User Approval

- After screening Source Host/IP, Destination Host/IP, Port, Service Type etc. VPN request will be finally approved by MD, UPDESCO.
- This approved request form will be handed over to DCO for creation of New VPN User.
- VPN user and password will be handed over to HOD/Nominated officer of respective departments personally only.
- It will be the responsibility of department Head / Nominated officer only that they have to change password immediately.
- Department user has to ensure the adherence of password security do's and don'ts.

Validity

- VPN user will be issued for a period of one year or till validity of the Security Audit Certificate, whichever is earlier.



- After completion of one year user has to follow the renewal process, again raise a fresh request duly signed from Additional Chief Secretary/Principal Secretary/Secretary/Special Secretary/HOD/Director/Joint Director of respective department and submit to UPDESCO for approval.

User Responsibility

- VPN Users has to make sure that the client system used for VPN connection is regularly scanned and updated with latest OS patches and anti-virus software.
- Once connected to UPSDC VPN, all traffic between the user's PC and UPSDC will be through VPN tunnel and user will have access to the authorized applications and Database servers only listed in the application form.
- Any change in the Intranet Web Applications/ hostname which are to be accessed through SSL VPN, has to be intimated to the VPN administration.
- Don't share password of your computer to unauthorized users (e.g., family members, friends and colleagues) from accessing information.
- Disconnect from the VPN when it is no longer needed.
- It is the responsibility of each VPN user that they do not allow any other individual to use their VPN account.
- If any violation of guidelines occurs this may include temporary/permanent suspension of accounts and/or network access.
- Ensure adherence of complex password policy.

Enforcement

The VPN user shall follow the policy.

Terms & Conditions:

1. The information provided by the User/Department should not be incorrect/false.
2. User shall be responsible for the contents / data uploaded to the servers through VPN connection. UPSDC is not responsible for the contents that are being accessed / upload by the user.
3. It is user's sole responsibility to use VPN account and shall be used only to accessing authorized servers/resources.
4. Password shall be set by user itself by physically presence in UPSDC and to keep the VPN user password confidential.
5. Password should be change on monthly basis by the authorized user/department by coming to UPSDC.
6. UPSDC is neither responsible nor accountable for any such misuse of the compromised VPN accounts or data changes. It's the user's whole sole responsibility.
7. The user's/ reporting officer's/ Department's responsibility that they inform on priority basis to disable the VPN account with immediate effect, when the user is transferred / relieved from the division/ responsibility.
8. User shall not indulge in any unauthorized activity or attempt to gain unauthorized access to other UPSDC servers or resources.
9. Its user's responsibility to install the Antivirus software with latest pattern/definition update periodically and OS patches in their system.
10. The VPN allocated/given to all the Departments will be withdrawn and renewed/reset on the request of the Department.
11. The VPN shall be issued in the name of the authorized & approved requester.
12. Its user's responsibility keeps the password confidential. UPSDC/UPDESCO is not responsible to maintain password security.
13. The password length should be of minimum 8 characters and the password should meet the complexity requirement.
14. Password must contain characters from all four categories
 - o English upper case characters (A to Z)
 - o English lower case characters (a to z)



- o Base 10 digits (0 to 9)
 - o Special characters (i.e. \$, %, # etc.)
15. Create different passwords for different accounts.
 16. Passwords should be changed on a periodic basis at least once in every month,
 17. Keep them to yourself. Avoid giving out your password to others. Once it's out of your control, so is your security.
 18. Do use a different password for different accounts.
 19. User passwords are sensitive, confidential information and must not be shared with others. Passwords are the first line of protection against threats to network security, whether threats originate internally or externally.
 20. Don't use personal information, like birthday dates, family member names, your nickname, birth date, spouse name, pet name, make/model of car, or favorite expression

☐ I have read and agree with policy and Terms & Conditions. (Please tick)

Department Requester	Department Approver (HOD)	UPDESCO Approver
Signature: Date: Stamp:	Signature: Date: Stamp:	Signature: Date: Stamp:

FOR DCO USE ONLY

1	Detail of Application	
2	Server IP	
3	Service Request No.	
4	Change Request No	
5	VPN User Name	
6	VPN Creation date	
7	Created By	
8	Date & Time	
REMARKS		

DCM, UPSDC

(With Date and seal)