State Data Center
Department of IT & Communication
Government of Arunachal Pradesh

VPN Access Request Form

1. Requestor Details

- Full Name:
- Department/Organization:
- Designation/Position:
- Contact Number:
- Email Address:

2. Purpose of VPN Access

- VPN user name (who will use this VPN):
- Reason for VPN Access:
  (e.g., Remote administration, system monitoring, accessing specific services, etc.)
- Detailed Description of Purpose:
- Duration of Access:

  Start Date:

  End Date (if applicable):
- Access Requirements:

  Specific systems or services to be accessed:

3. Access Details

- VPN Access Start Date:
- VPN Access Expiry Date:

4. Terms and Conditions

- I hereby agree to abide by the VPN access policies of the State Data Center. Misuse of VPN access will result in termination of access rights and possible disciplinary action.

5. Requester Department HoD: (Director/ Secretary/ Undersecretary)

- Name:
- Designation:
- Signature with Seal:
- Date:

State Data Center
Department of IT & Communication
Government of Arunachal Pradesh

For Department of IT & Communication,

Approved by:

Signature:

Name:

Designation:

Note:

1. Minimum 2 working days required to address VPN request.
2. VPN access details/credential need to be collected by user from State Data Center by showing this form and ID proof during working hours.
3. VPN can be access only from windows system.
4. Only IPSec VPN will be provide.

State Data Center
Department of IT & Communication
Government of Arunachal Pradesh

VPN Access Policy

1. Purpose

The purpose of this policy is to establish security protocols for Virtual Private Network (VPN) connections to the State Data Center's network. This policy is designed to protect the data center's systems and data from unauthorized access and ensure that all VPN connections are managed in a secure manner.

2. Scope

This policy applies to all employees, vendors, and any third-party users who require remote access to the state data center's internal network via a VPN connection.

3. Access Eligibility

VPN access is granted based on job requirements and is limited to authorized personnel. The following categories of users may be eligible for VPN access: VPN access request should be send with approval of HoD/Director/Special/Under Secretary/CEO.

- State government employees needing remote access to internal systems.
- Contractors or third-party vendors engaged in approved state projects.
- System administrators and network engineers for system maintenance and monitoring.

4. VPN Access Requirements

- **Authorization:** All VPN access must be authorized by the relevant department head and approved by the Project Incharge or data center manager.
- **Request Process:** Users requesting VPN access must submit a formal VPN access request form detailing the need for access, the services required, and the duration of access.
- **Access Duration:** VPN access is granted for a specific period based on the request, and the access must be renewed if required beyond the initial duration.

5. Security Protocols

- **Encryption:** VPN connections must be encrypted using industry-standard encryption protocols (e.g., IPsec, SSL/TLS).
- **Authentication:** Multi-factor authentication (MFA) must be enabled for all VPN users to ensure secure access.
- **Access Control:** Users will be granted access only to the systems and services necessary to fulfill their role. Any attempts to access unauthorized systems will result in immediate termination of access and possible disciplinary action.
- **Device Security:** All devices connecting to the VPN must have up-to-date antivirus software, firewalls, and security patches. Devices that do not meet security requirements will be denied access.

- **IP Whitelisting:** VPN connections may only be made from whitelisted IP addresses when possible, to limit exposure to unauthorized networks.

6. Monitoring and Auditing

- All VPN connections will be logged and monitored. Logs will include details such as the user's identity, source IP address, connection time, and the resources accessed.
- Audits will be conducted periodically to ensure compliance with the VPN access policy. Any suspicious activity will be investigated promptly.

7. User Responsibilities

- Users must not share VPN credentials with any other individual.
- Users must report any security breaches, such as unauthorized access or stolen credentials, immediately to the network/security administrator.
- Users must follow all relevant security guidelines and best practices when accessing the state data center's network via VPN.

8. Termination of Access

VPN access will be terminated under the following conditions:

- When the user's access period expires.
- When the user's employment or contract ends.
- If the user violates the VPN access policy.

9. Consequences of Policy Violation

Any violation of this policy may result in disciplinary action, including suspension or revocation of VPN access privileges, termination of employment, and/or legal action.

Policy Review and Updates

This VPN Access Policy will be reviewed annually or whenever significant changes in network security standards or operational procedures occur.