Virtual Private Network (VPN) Remote Access Usage Policy

Purpose

The purpose of this policy is to define user expectations and capability for remotely connecting to INDIAN INSTITUTE OF ASTROPHYSICS (IIA), Bangalore campus network from various host devices via the Internet. These principles are designed to minimize unnecessary exposure and damage to IIA information and information systems. Inappropriate exposure and damages may include the loss of sensitive or confidential data, intellectual property, mitigation of malware infestation, damage to public image, or damage to critical internal systems and services.

Scope

This policy applies to all remote access connections with an IIA owned mobile device, virtual host, laptop, workstation, server or cluster used to do work, e.g., all employees, students, collaborators, interns, project associates, consultants and vendors. Remote access implementations that are covered by this policy include various technologies, and are not limited to only, RDP, SFTP, IPSEC, SSH, etc.

Policy

IIA employees and authorized third parties (collaborators, interns, project associates, vendors, etc.) may utilize the benefits of the VPN to access IIA computing resources to which they have been granted access. VPN software and support is available through IIA IT Support.

1. IIA VPN services are to be used solely for IIA academic and research support purposes. All users are subject to monitoring and auditing of VPN usage.

2. VPN services will be terminated immediately if any suspicious activity is detected.

3. VPN profiles are created upon request and final approval. The approval process MUST be initiated by the user or through his/her immediate supervisor and final approval granted through Computer Committee Chairman. The signed VPN Request form must be submitted to IIA IT Support, and must be in compliance with VPN Remote Access Use Policy. Accounts will not be issued until this process has been completed. The user is required to fill the duration of the VPN use period after which the VPN access will be terminated for use by the user.

4. IIA campus network access will be limited ONLY to the resources to which users have been approved. Open and / or unlimited access for these

accounts will not be permitted.

5. Users will be automatically be disconnected from the IIA network after a period of inactivity, per the current user's security profile. The user must then logon again to re-authenticate in order to regain a connection to the network.

6. The VPN tunnel will be configured to mitigate potential 'back-doors' to the campus network and associated resources. Therefore all remote access connections to the IIA campus network will require traffic to and from other internet sites to process through the VPN connection. Dual (split) tunneling is NOT permitted, e.g., two separate connections to the internet.

7. To accommodate regularly scheduled maintenance, interruption of remote connectivity to campus resources service will occur. VPN service interruption will be communicated prior to maintenance requirements in order to accommodate users planning. Additional emergency downtime may be scheduled and announced as needed.

8. VPN profiles are typically created per current IT service level requirements. Urgent requests will be reviewed on a case-by-case basis.

Accountability

Failure to abide by the requirements of this policy and / or any procedures that are developed to implement this policy may result in termination of the user's VPN privileges. Users may also be subject to sanctions, including the loss of computer and / or network access privileges, disciplinary action, suspension. The immediate supervisor/signing authority (guarantor) for the student/intern/project associate will also be held accountable for any misuse of the VPN facility and any further VPN access request from him/her will not be entertained in future.