Remote Access Request Policy

Virtual Private Network (VPN)
The VPN network provide secure, remote access to select services on the University network. This service is provided to allow individuals the capability to perform critical responsibilities while away from the campus.

General Policy
Remote access to the campus network is provided as a convenience to staff and faculty members. All users must follow the University of Redlands Policy for Responsible Use of Information Technology. When VPN access is granted, participants are required to sign the request form indicating that they are in agreement with all applicable University policies.

Service Terms and Conditions
Requestors must demonstrate an academic or business need for remote access to the University Network. Use of this service in the performance of activities unrelated to the mission of the University is strictly prohibited.

VPN is a user-managed service, which means that off-campus users of this technology are responsible for selecting an Internet Service Provider (ISP), coordinating installation with their ISP of any required software, and paying associated fees.

Additionally,

1. It is the responsibility of those with VPN privileges to prevent unauthorized access to Redlands network from their remotely connected computer, be it at home or some other location.
2. Users will be authenticated through their RedlandsID and password.
3. All computers remotely connected to University of Redlands network **must**:
    a. Use the most current anti-virus protection.
    b. Keep computers updated with the latest critical operating systems patches
    c. Use compatible firewall protection. Information regarding compatible firewalls may be obtained from Information Technology Services (ITS).
    d. The remote connection must not bridge a remote network to the University's network. Only a single computer is allowed to remotely connect to the University's network.
4. When remotely connected to University network, users will adhere to the same University policies and regulations that apply to on campus usage. This includes all of the University's Information Technology Services policies, including its Acceptable Use Policy.
5. Remote users may be disconnected after 15 minutes of inactivity. Pings or other artificial means used to bypass this time limit are strictly prohibited.
6. Remote access total connection times are limited to 8 hours.
7. All requestors must read and agree to these terms and condition before remote access is granted.
8. Data collected, stored, backed up, processed or accessed using this service must be protected according to University policies and procedures.
9. **Confidential University data must not be stored on privately owned systems.**
10. At the end of employment, any contractual arrangement, or cessation of the individual's remote access, all University data and intellectual property must be removed from off-campus systems.
11. Information Technology Services may annually review remote access requests for validation and audit purposes.

Failure to Adhere to Policy
Any violation of the University network or Policy of Responsible Use of Information Technology, the University will take action deemed necessary, including disconnection of service and denial of future requests.

Limits of Service
The University of Redlands maintains networks resources for the use of its students, faculty and staff in pursuing academic endeavors. Remote access to these resources is provided as a convenience; however, the University may limit or remove access at any time.

Updated February 2020