In an effort to keep confidential data secure, while also understanding that our changing culture requires work to be performed remotely, CSULB provides remote access to faculty and staff with appropriate approval. This document outlines procedures and protocols for providing remote access to faculty and staff.

### General

1. It is the responsibility of CSULB employees to ensure that all possible measures have been taken to secure the remote computer (such as installing hardware and software firewalls) and have the most recent operating system and application patches. These practices must use the most up-to-date anti-virus software, keep virus definitions up to date, and run regular scans. This includes personally owned computers used for CSULB business.

2. All CSULB faculty and staff will be granted remote access privilege as part of their normal network access. **General access to the Internet for recreational use by immediate household members through the CSULB Dial-in Modem Network is discouraged.** The CSULB employee is responsible to ensure the family member does not violate any CSULB polices, does not perform illegal activities, and does not use the access for outside business interests. The CSULB employee bears responsibility for the consequences if the access is misused.

3. Students will not be granted remote access privileges.

4. Affiliates who require remote access privileges will be granted access on a case by case basis (refer to Remote Access Request Form).

5. Dial-up connections will only have the same access as internet users.

6. No devices or software may be installed that allows remote access to the CSULB network such as modems, wireless access points, or VPN servers. All remote access will be provided centrally by Information Technology Services.

### Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication.

2. At no time should any CSULB employee provide his or her login or email password to anyone, not even family members. ITS employees will never ask for a Remote User’s password.

3. Remote Users must ensure that their University-owned or personal computer or workstation, which is remotely connected to the University network, is not connected to any other external network at the same time, other than a Private Network under the user’s control.

4. Reconfiguration of a remote user’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

5. All hosts connecting to the internal system not generally available to all internet users will connect through a VPN session to the university’s centrally managed VPN server unless special dispensation is requested and granted.

6. External contractors may be granted access to internal hosts without using a VPN session if there is a business reason and special dispensation is requested and granted. Only access from static IP addresses will be granted.

7. Only supported remote control software will be allowed to communicate from the VPN server to internal hosts unless specifically requested and approved.