VPN ACCESS REQUEST

Employee Name: _____ Date: _____

Datatel ID/W#: _____ Title: _____

Work Location: _____ Campus Phone #: _____

Manager's Name: _____

Reason VPN access is necessary: _____

_____

_____

Employee Signature: …….. Date: _____

Manager's Signature: …….. Date: _____

Assistant Vice Chancellor of ITS Signature: …… Date: _____

You may fax to YCCD IT Dept. at ext. 6306 (no cover sheet is necessary), or send through campus mail. **Print**

Virtual Private Network (VPN) Procedure

1.0 Purpose
The purpose of this procedure is to provide guidelines for remote access IPSec or SSL Virtual Private Network (VPN) connections to the YCCD network.

2.0 Scope
This Procedure applies to all YCCD employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the YCCD network.

3.1 Procedure
Approved YCCD employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally -

1. VPN user access is granted by the YCCD Information Technology department. VPN access requests should be originated through the department dean/manager or appropriate designated managerial assistant.
2. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to YCCD internal networks.
3. IPSEC VPN use is to be controlled using public/private key system or a strong passphrase combined with user authentication.
4. When actively connected to the YCCD network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
5. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
6. VPN gateways will be set up and managed by YCCD Information Technology Networking/Telecom Department.
7. All computers connected to YCCD internal networks via VPN or any other technology must use up-to-date anti-virus; this includes personal computers.
8. Users of computers that are not YCCD-owned equipment must configure the equipment to comply with YCCD's VPN and Network Procedures.
9. Only YCCD approved VPN clients may be used.
10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of YCCD's network, and as such are subject to the same rules and regulations that apply to YCCD-owned equipment, i.e., their machines must be configured to comply with YCCD's Security Procedures.
11. YCCD VPN access should only be used for YCCD and related entities work. VPN connections should be disconnected when users are not performing work related functions.

4.0 Enforcement
Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
IPSec gateway	A device in which VPN connections are terminated.

6.0 Revised Date: *7/22/2015*