Information Security - Remote Access

1.0 Purpose and Scope

The objective of this Administrative Regulation is to control access to YCCD information and systems when connections are made to those systems from a remote location.

This is one of a series of information security Administrative Regulations maintained by the District Information Technology Services (ITS) department designed to protect YCCD information systems.

2.0 Remote Access

All connections into and out of the internal network must be documented and managed by District ITS. Remote access is not automatically provided to all personnel and must be requested and approved as described below. The exception to this is access to the Student Information System (SIS) through connectColumbia, PiratesNet or StaffNet using an Internet browser. Access to connectColumbia, PiratesNet or StaffNet is authorized for both staff and students, based on their job function and role, using assigned credentials and passwords.

Users must use established remote access mechanisms or gateways to District systems. Aside from connectColumbia, PiratesNet or StaffNet, the ONLY approved connection method is used to gain access to YCCD systems is an SSL VPN client account (supplied by District ITS).

Remote access is prohibited from any public or shared computer or Internet kiosk.

Users may not establish new remote access systems or methods unless approval has been granted by the Assistant Vice Chancellor of Technology. District ITS Management will audit all remote access quarterly.

2.1 Requests for Remote Access

Users create help desk tickets to request remote access. Refer to the ITS-AR-1501 *Access Control* for further information.

2.2 Approvals for Remote Access

YCCD Remote access is granted on a case by case basis for district employees with a compelling business need. A compelling business need shall be defined as a process or task that is a requirement of your job duties, and if not completed would have ramifications or fiscal impact on the college or district.

Examples

- Need to access sensitive or confidential files from a location outside of the district.
- Remote access to servers and network resources for administration or

maintenance.

- Monitoring of Critical system processing.

Remote access for YCCD employees must be approved by the Assistant Vice Chancellor of Technology or designee. College Staff requesting remote access must also have their request approved by their college president.

2.3 Access Controls for Remote Connections

Remote access sessions will be automatically disconnected after 30 minutes of inactivity.

Personal firewall software must be installed on all YCCD or employee-owned computers with direct connectivity to the Internet that are used to access a District network. Anti-virus software must also be installed and must include the most recent software updates and virus profiles.

Any remote access connection that has been established for a vendor, business partner, or other third party for purposes of support must be immediately deactivated once no longer in use by the appropriate ITS staff.

2.4 Transmission Over Networks

If YCCD *Restricted* data is to be transmitted over any communications network, it must be sent only in encrypted form. Networks include YCCD email mail systems, connections using the Internet, and supplied YCCD remote access systems. All such transmissions must use software encryption approved by the District ITS department. Refer to the ITS-AR-1504 Data Classification for further information.

2.5 Payment Card Industry Considerations

YCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). Where cardholder data is present, remote access to those systems must incorporate two-factor authentication. This refers to network-level access originating from outside the YCCD network to the YCCD network by employees and third parties.

For personnel accessing cardholder data via remote-access technologies, copy, move, and storage of cardholder data onto local hard drives and removable electronic media is prohibited unless explicitly authorized by the Assistant Vice Chancellor of Technology for a legitimate business need.