# ADMINISTRATIVE REGULATION 3729

## COLLEGE OF THE REDWOODS

### INFORMATION SECURITY-REMOTE ACCESS

#### Purpose and Scope

The objective of this Administrative Regulation is to control access to the district’s 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 (IT) department designed to protect the district’s information systems.

#### Remote Access

All connections into and out of the internal network must be documented and managed by District IT. Remote access is not automatically provided to all personnel and must be requested and approved as described below.

Users must use established remote access mechanisms or gateways to District systems. Approved connection methods are used to gain access to the district’s systems: an SSL VPN client (supplied by District IT).

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 as noted below.

All remote access will be audited annually by District IT Management.

##### Requests for Remote Access

Users create service desk tickets to request remote access.

##### Approvals for Remote Access

General remote access: For college staff, remote access must be approved by the college President or designee. For District Services, remote access must be approved by the IT Director or designee.

New remote access methods: District IT Director must approve any new remote access method or system.

##### Access Controls for Remote Connections

Remote access sessions will be automatically disconnected after 15 minutes of inactivity.

Personal firewall software must be installed on all district 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 IT staff.

##### Transmission Over Networks

If district *Restricted* data is to be transmitted over any communications network, it must be sent only in encrypted form. Networks include the district email mail systems, connections using the Internet, and supplied district remote access systems. All such transmissions must use software encryption approved by the District IT department.

##### Payment Card Industry Considerations

**COLLEGE OF THE REDWOODS** 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 district’s network to the district’s 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 College President or designee for a legitimate business need.