VPN Account Configuration Request

Authorization signatures must be present before adding or altering VPN accounts.

Page 1 of 2: Request information and Authorization Signatures

Configuration Type *New. Reconfigure Existing. Disable. or Delete*	

User Full Name *First, Last*		Employee ID	
User Organization	*Peralta site, or Company*	select or type	
	Phone#		
	Email		
Required Internal Resources *Applications/Systems, Server, and/or IP Address*			
Purpose			
Term *Days, weeks, months, specific dates, or duration of employment or contract*			
Authorizing Manager *See page 2 for area managers.* *Requestor must be Peralta manager*	*Name*		
	Position		
	Phone#		
	Email		
	Signature		
Request Date			

Authorizing IT Manager Name	
Authorizing IT Manager Signature	

All authorizations must be present before request can be can be executed.

VPN Account Configuration Request

Authorization signatures must be present before adding or altering VPN accounts.

Page 2 of 2: To be completed by technician

Technician Name		
Service Date		
Remote Access Classification *General Use, Specified Systems Use, IT Admin Basic or IT Admin ERP.* *To be determined by IT staff, based on Items 3, 4, and 7, above.*		
VPN Type *WebVPN, 3030, or 5505* *To be determined by IT staff, based on Items 3 and 4, above.* *5505 (certificate) accounts are created only after user's need for system administration is confirmed. Contact requester for further info if necessary.*		
Account Name		
Access Parameter	*WebVPN* *AD group name* *3030* *local group name* *5505* *local ID & certificate name*	

De-activation *Deactivation Codes:* *Expired* *not currently used* *Terminated* *Contract or Employment is ended*	*Authorized by*	
	Deactivation Code	
	Email	

The following information, from the Remote Access Policy, is intended to assist site staff in identifying the required site Authorizing Manager.

1. Remote Access classifications are:

General Use	Allows access to specific resources through WebVPN.
Specified Systems Use	Allows access to specific systems through IPSEC VPN.
IT Administration – Basic	Allows access to site networks and systems through IPSEC VPN.
IT Administration – ERP	Allows access to networks and systems comprising the ERP back end through two factor authentication and IPSEC VPN.

Connection to all remote access systems is password protected and encrypted.

2. Authorization by the following Enterprise Managers is required for Remote Access:

General Use	IT Resource Users who have already been authorized according to the Account Access Policy are automatically provided with General Use Remote Access.
Specified Systems Use	Management for area served by the specified system. For example, Remote Access for the Library Online Catalog system is authorized by the librarian currently managing that system, as designated by the District Librarian Group.
IT Administration – Basic	Site Management and District Information Technology Management.
IT Administration – ERP	District Information Technology Management.