KERN COUNTY SUPERINTENDENT OF SCHOOLS OFFICE

PERSONNEL

VIRTUAL PRIVATE NETWORK

The purpose of this policy is to provide guidelines for remote access virtual private network (VPN) connections to the Kern County Superintendent of Schools Office business office network.

This policy applies to permanent employees, temporary employees, and other workers including all personnel affiliated with third parties (e.g., school districts) using VPNs to access the business office network. This policy applies to all implementations of VPN services.

Approved third parties may use services provided by the VPN in accordance with the rules and guidelines contained herein, as well as those in the Kern County Superintendent of Schools Office Acceptable Use Policy for Office Supplied Computer, Network, Internet, E-mail, and other Communication Devises. VPN services are accessed through the user's ISP. The user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees for that service.

It is the responsibility of users with VPN privileges to ensure that unauthorized users are not allowed to access the Kern County Superintendent of Schools Office internal networks. The VPN client parameters may not be changed by the user for any reason, without express written instruction from the Kern County Superintendent of Schools Office VPN technical support. VPN gateways will be set up and managed by Kern County Superintendent of Schools Office network operational groups.

All computers connected to the Kern County Superintendent of Schools Office internal networks via VPN or other technology must use the most up-to-date anti-virus software, according to the office-approved standard. Approved anti-virus software is Network Associates' McAfee Antivirus, version 7.1 Enterprise, Superdat version 4363 (as of 06/01/04) and updated weekly. This software is available to all departments directly affiliated with or operated by the Kern County Superintendent of Schools Office.

VPN users will be automatically disconnected from the Kern County Superintendent of Schools Office VPN after thirty minutes of inactivity. The user must then logon to reconnect to the network. Pings or other artificial network processes may not be used to keep the connection open.

Users of equipment that is not Kern County Superintendent of Schools Office owned must configure the equipment to comply with the Kern County Superintendent of Schools Office VPN and network policies. All operating systems must run the latest security updates as provided by the maker of the operating system. Only Kern County Superintendent of Schools Office supplied VPN client software and hardware may be

used. By using VPN technology with non-Kern County Superintendent of Schools Office equipment, users must understand that their machines are a *de facto* extension of Kern County Superintendent of Schools Office's network, and as such, are subject to the same rules and regulations that apply to office-owned equipment, i.e., machines must be configured to comply with the office security and acceptable use policies. Any VPN user found to have violated this policy is subject to termination of VPN privileges.