

CDI	Information Security Policy
------------	--

To: CDI Employees

No.: ISO-03

From: Information Security Office (ISO)

Issued: August 1, 2004

Subject: Remote Access Policy

Expires: When Superseded

Policy

It is the policy of the California Department of Insurance (CDI) to provide remote access to CDI systems and information to employees when there is a business need (e.g. teleworkers, users who travel or work away from a CDI office, etc.) Users connecting remotely to CDI systems must do so with CDI owned and maintained equipment.

Users may connect remotely using non-CDI equipment when using Outlook Web Access. Please note system requirements in "Remote Access System Security and the User" below.

Requests for exceptions to this policy must be made to the Information Technology Division (ITD) and will be reviewed and evaluated by the appropriate ITD supervisor on a case-by-case basis.

Purpose

To protect the CDI network from malicious codes, hacker penetrations, viruses, Trojans and other vulnerabilities.

Authorization for Remote Access to CDI Systems

Remote access to CDI systems must be through CDI approved remote access methods.

Approved Remote Access Methods

Cisco VPN is the only approved remote access connection option currently in use by CDI.

Unapproved Remote Access Methods

To ensure that the security of CDI information or systems will not be compromised, users who have on-line access to another agency's information (i.e. another state or federal agency) while working in a CDI office, may not connect remotely to another agency unless the agency has given permission to CDI for its users to access the agency's information remotely.

Remote Access Information Confidentiality

All information obtained using remote access to CDI systems is subject to the confidentiality and disclosure provisions of [SAM Section 5320.5](#).

Remote Access System Security and the User

All employees connecting remotely to CDI systems must have the latest service packs and updated anti-virus software installed and running on the personal computer (PC) used to connect to the CDI systems. The PC used to connect remotely to CDI systems must not be connected to any home, business, or other public agency network, Local Area Network (LAN) or Wide Area Network (WAN) while connecting remotely to CDI systems.

Remote users connecting to CDI systems through a Digital Subscriber Line (DSL), cable modem, or any other high bandwidth open line connection must have some type of firewall installed on the PC in order to provide the necessary layer of protection needed. Any updates or patches to the firewall must be the latest version available and must be applied immediately. Security on the firewall is to be set to "high".

De-activation of Remote Access

Managers and supervisors are responsible for immediately notifying the ITD help desk to de-activate the remote access for a CDI employee who is leaving CDI employment or who no longer requires remote access.

When remote access is cancelled or the employee leaves CDI's employment, managers and supervisors must collect all remote authentication devices (e.g. tokens, smartcards, laptops, etc.) from the employee.

Request to Use Non-CDI Owned Equipment for Remote Access

Each request must be reviewed and approved or denied by the employee's supervisor or manager, ITD and ISO. At a minimum, any device that is used to connect to the CDI network must have the latest operating system security

patches applied and the most current virus patterns loaded. Please contact the ITD help desk to verify compliance with this policy.

Inquiries

Please contact the ISO at 916-492-3256 or 916-492-3353 if you have any questions regarding this policy.

Archie Alimagno, Information Security Officer