

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

To: CDI Employees

No.: ISO-04

From: Information Security Office (ISO)

Reissued: July 3, 2006

Subject: Wireless Devices Policy

Expires: When Superseded

Policy

California Department of Insurance (CDI) does not allow the use of any wireless devices such as wireless access points, Blackberry devices, personal digital assistants (PDAs) with wireless modems, laptop computers with wireless modems, or any wireless networks to be used within any CDI facility. This policy also includes the use of cell phones for data transmission or retrieval. Wireless technology in its current state is inherently open and subject to security vulnerabilities.

However, CDI does permit the use of wireless devices, such as cell phones, PDAs, Blackberry devices, workstations or laptops provided they are not using the CDI network to directly transmit data or voice to mobile users. Commercial internet service providers (ISPs) are used for these non-CDI network services. If business requirements dictate the need for using wireless connectivity for your laptop or other wireless device, CDI will procure the necessary standard equipment to ensure that security is enabled for the device(s). A VPN must be used if a user will access network resources (i.e. h:\ or shared drives and files).

Purpose

To protect CDI's network from being compromised and to ensure that CDI personal, confidential and proprietary information is protected and not disseminated without proper approval or user knowledge.

Procedure

The Information Technology Division (ITD) and ISO will continue to develop necessary procedures, which will address secure wireless configuration, implementation, and deployment to mitigate risks to CDI networks. CDI staff will use the approved configuration for wireless devices if they wish to use wireless technology in the field or their home. Using wireless technology in the CDI location will be approved by ITD and ISO on a case by case basis.

* Virtual Private Network (VPN)

Things to Consider in Setting up a Wireless Router at home:

1. Change the default SSID: Your wireless devices have a default SSID (Service Set Identifier) set by the factory. The SSID is the name of your wireless network, and can be up to 32 characters.
2. Disable SSID broadcast: By default, most wireless networking devices are set to broadcast the SSID, so anyone can easily join the wireless network with just this information. But hackers will also be able to connect your network. You can configure the devices on your network to automatically connect to a specific SSID without broadcasting the SSID from your router.
3. Change the default password: For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory.
4. Enable MAC address filtering: Most routers give you the ability to enable MAC (Media Access Control) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify only the computers in your house to access your wireless network. It would be very difficult for a hacker to access your network using a random MAC address.
5. Enable Encryption: Encryption allows protection for data that is transmitted over a wireless network. Wired Equivalency Protocol (WEP) and Wi-Fi Protected Access (WPA) offer different levels of security for wireless communication. WEP is currently the most widely used level of encryption and is supported by more devices than WPA.
6. Enable the Firewall on your workstation/laptop at home and keep your virus protection and Microsoft updates current on your systems.

Inquiries

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