I. PURPOSE

CRT Labs provides access to the vast information resources of the Internet to help you do your job faster and smarter, be a well-informed employee, and assist in providing a greater work-life balance. The facilities to provide that access represent a considerable commitment of company resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to help you understand our expectations for the use of these resources and to help you use them wisely. While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy.

II. PHILOSOPHY

First and foremost, the Internet is a business tool, provided to you at significant cost. That means we expect you to use your Internet access for business-related purposes, i.e., to communicate with clients and vendors, to research relevant topics and obtain useful business information. We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. All existing company policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality. Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the company and expose it to significant legal liabilities. The chats, news groups and email of the Internet give each individual Internet user an immense and unprecedented reach to propagate company messages and tell our business story. Because of that power we must take special care to maintain the clarity, consistency and integrity of CRT Labs image and posture. Anything any one employee writes in the course of acting for the company on the Internet can be taken as representing the company's posture. That is why we expect you to forgo a measure of your individual freedom when you participate in chats or news groups on company business, as outlined below.

While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using the Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. Any employee using the Internet can be held accountable for any breaches of security or confidentiality.

Certain terms in this policy should be clearly understood. Company includes our corporate and division offices. Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in a Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. Graphics includes photographs, pictures, animations, movies, or drawings. Display includes monitors, flat-panel active or passive matrix displays, monochrome LCD's projectors, televisions and virtual-reality tools. '

All employees granted Internet access with company facilities will be provide with a written copy of this policy. All employees must sign the following statement to be placed in their employee file:

"I have received a written copy of my company's Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the company's security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to dismissal or even criminal prosecution."

III. POLICY

A. Management and Administration

The company has software and systems in place that can monitor and record all Internet usage. We want you to be aware that our security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, news group or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or -her Internet usage. Our Information Service Manager and Vice President of the People Department will review Internet activity and analyze usage patterns, and they may choose to use this data to assure that company Internet resources are devoted to maintaining the highest levels of productivity.

1. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

2. The display of any kind of sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored distributed, edited, or recorded using our network or computing resources.

3. The company uses independently-supplied software and data to identify inappropriate or sexually-explicit Internet sites. This software may block access from within our networks to all such sites that we know of. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

4. This company's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulation of any state, city province, or other local jurisdiction in any material way. Use of any company resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

5. Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

6. No employee may use company facilities knowingly to download or distribute pirated software *or* data.

7. No employee may use company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

8. No employee may use the company's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

9. Each employee using the Internet facilities of the company shall identify himself or herself honestly, accurately and completely (including one's company affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

10. Only those employees or officials who are duly authorized to speak to the media, to analysts or the public gatherings on behalf of the company may speak/write in the name of the company to any news group or chat room. Other employees may participate in news groups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this company, the employee must refrain from any unauthorized political advocacy and must refrain from the

unauthorized endorsement or appearance of endorsement by the company of any commercial product or service not sold or serviced by this company, its subsidiaries or its affiliates. Only those managers and company officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the company may grant such authority to news group or chat room participants.

11. The company retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

12. Employees are reminded that chats and news groups are public forums where it is inappropriate to reveal confidential company information, customer data, trade secrets, and any other material covered by existing company secrecy policies and procedures. Employees releasing protected information via a newsgroup or chat-whether or not the release is inadvertent-will be subject to all penalties under existing data security policies and procedures.

13. Use of company Internet access facilities to commit infractions such as misuse of company assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property are also prohibited by general company policy, and will sanctioned under the relevant provisions of the human resources policies and procedures manual.

14. Employees may use their Internet facilities for non-business research or browsing during the lunch hour, or outside of work hours, PROVIDED THAT ALL OTHER USAGE POLICIES ARE ADHERED TO.

B. Technical

1. User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password of ID for an Internet resource must keep that password confidential. Company policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.

2. Employees should schedule communications-intensive operations such as large file transfers, video downloads, mass emailings and the like for off- peak times (During lunch hours or after hours).

C. Security

1. The company has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the company's networks. Any employee who attempts to disable, defeat or circumvent any company security facility will be subject to immediate dismissal.

2. Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connections to any outside computer can be used by an attacker to compromise any company network to which that computer is attached. That is why any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from company's internal networks.