



## CIPA Compliance

### Children's Internet Protection Act

#### The CIPA Act

In December 2000, the US Congress enacted the Children's Internet Protection Act (CIPA) to respond to the issue concerning Internet access in schools and libraries. CIPA requires that schools and libraries which receive funding under the E-Rate program must have an Internet Safety Policy in place that addresses the safety and security of minors online.

Cyberoam, the Integrated Internet Security Appliance, assists CIPA compliance for schools and libraries through its powerful content filtering, allowing them to enforce an Internet safety policy that blocks and filters Internet access in accordance with CIPA requirements.

Its unique Identity-based security policy enforcement offers complete visibility into individual users; students, faculty, and administrators, responding specifically to the challenge of multiple users utilizing shared systems, and the need of providing policy based on user identity and group membership. In addition, Cyberoam offers comprehensive protection against Internet threats with a complete set of integrated security solutions on a single platform.

#### CIPA Guidelines

- Schools and libraries subject to CIPA may not receive the discounts offered by the E-Rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors, for computers that are accessed by minors.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
- Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them.

#### CIPA Compliance with Cyberoam

- Cyberoam offers extensive content filtering through its site database with millions of categorized sites. It identifies student activity by the user name instantly, enabling institutions to monitor online activity with ease.
- Blocks Objectionable Sites: WebCat, Cyberoam's automated site categorization engine, carries a continuously updated (by Cyberoam's WebCat research team) site database of millions of sites in over 60 comprehensive categories, including Pornography, Adult Content, Alcohol, Tobacco, Crime and Suicide, Drugs, Gambling, Nudity, Violence, Weapons and more. Additionally, there is a category for URLTranslationSites which contains a list of web proxies and CGI proxies that are often used by students and other



users to bypass web content filtering products and services. This protects schools and libraries from objectionable surfing and downloads. Administrators have the ability to add sites to the blocked site list, customizing Cyberoam to meet their school's requirements.

### Prevents Personal Information Leakage

Cyberoam prevents students from revealing personal, sensitive or confidential information via email, chat rooms, instant messaging applications, and more, protecting students from predatory activity.

### Preventing Site Filtering for Academic Purposes

Cyberoam's unique Identity-based security allows administrators to create Internet access policies based on user, group or department, ensuring that academic sites are not blocked for the relevant groups or users. Policies can even be set to give temporary access to sites for project-based research.

### Monitoring and Reporting with Student Name

Cyberoam's Identity-based reporting offers complete and instant visibility into student activity through its reporting, which presents the username rather than just the machine's IP address. This allows administrators to identify the students instantly despite the fact that multiple users may share the same systems. Cyberoam reports are delivered in user-friendly CSV, graphical and tabular formats that offer insights into user behavior and attacks on the network.

### Cyberoam - Complete Internet Security

In addition to ensuring that schools and libraries comply with CIPA requirements, Cyberoam offers complete protection from internal and external threats like viruses, worms, Trojans, DoS attacks, spyware, phishing, pharming and more. It protects the institutions from internal threats that result in legal liability, due to illegal P2P file sharing, data leakage and data loss, issues of sexual harassment and more.

Cyberoam offers a complete set of security features Identity-based Firewall, Virtual Private Network (VPN), Gateway Anti-virus and Anti-spam, Intrusion Detection and Prevention (IDP), Content Filtering, in addition to Bandwidth Management and Multiple Link Management.

### Cyberoam Identity-based Security

Cyberoam's unique Identity-based security offers complete visibility into individual users, allowing schools and libraries to protect students while securing the institution from issues of legal liability arising out of internal threats. In addition, it plays a central role in securing E-Rate funding for their Internet access and Internet connection investments.