ACTION, TO SHARE

LOS ANGELES UNIFIED SCHOOL DISTRICT
Office of the Chief Information Officer

DISTRIBUTION: All Schools and Offices

SUBJECT: BULLETIN NO. K-24 (Rev.)
LAUSD FIREWALL POLICY

DATE: November 4, 2002

DIVISION: Information Technology

APPROVED: MARGARET A. KLEE, Chief Information Officer

ROUTING
Administrators
Loc. District School
Support Directors
Instr. Tech. Application
Facilitators

For further information, please call Patrick Luce, Coordinator, Network Security, (213) 241-1343 or email patrick.luce@lausd.net.

This revision replaces the bulletin of the same number dated February 15, 2002. The content has been updated to reflect current procedures.

I. BACKGROUND

As classrooms and offices continue to become electronically connected together for the exchange of information, it is critical that both school and office Local Area Networks (LANs) and the District's Wide Area Network (WAN) are protected from malicious activity. The District and its employees are responsible for the integrity and security of the data that is maintained and to ensure that private information, such as student and staff records, is adequately protected. There are legal risks for failure to implement and maintain reasonable safeguards for data security and the privacy of information. Additionally, security breaches and disclosure of confidential information would violate the relationship of trust the District has with its students, staff, and the public.

Several security protection measures have already been taken to protect the District's network and comply with applicable laws. Examples include District-wide licensing and implementation of anti-virus software, Internet content filtering, elimination of extraneous points of entry into the District's network, and enhancement of the District's "firewall" protection.

One of the critical elements for network protection is the "firewall." A firewall is a set of interrelated programs that protects LAUSD's network from users on other networks. The District's firewall prevents outsiders from accessing the District's private data resources. Firewalls have "ports" that can be opened to let specific types of traffic through, or closed to stop traffic. While ports are opened with the intent of permitting authorized legitimate traffic, hackers have become adept at developing mechanisms for using these points of entry to gain access to networks for unauthorized and often malicious or illegal purposes.

The Firewall is also used to block access by users on the District's network to specific computers or services on the Internet that make the District vulnerable to viruses or other risks. The District continues to evaluate and, if necessary, eliminate ports and services that pose a risk to network resources or threaten compliance with state and federal safety and privacy laws.

II. OBJECTIVES

Policies and procedures are being put into place that are intended to strike a reasonable balance between the availability of information to the Internet and the security of the District's network as a whole. These policies and procedures will:

- Enable ITD to configure District firewalls to provide the District WAN with the greatest amount of protection from intruders.
- Enable the District to protect sensitive information and comply with legal requirements.
- Allow for the dissemination of information necessary to the public, or information necessary for legitimate District purposes, through the District's Firewall(s).
- Enable ITD to evaluate and continuously monitor the security of all District servers accessible from the Internet.

III. POLICIES AND PROCEDURES

A. Acceptable Services Policy

Network based information services accessible through the District's firewall fall into three categories:

1. Disallowed Services
2. Services Limited to the Central District
3. Limited Services Allowed to Sites

1. Disallowed Services.

Some network-based services are inherently insecure and susceptible to hackers. A list of current examples may be found in Attachment B. A wide variety of ways to exploit these services, such as to gain unauthorized access to a network or do harm to systems and data, are known and widely advertised. Allowing these services to be passed through the District's firewall from the Internet would be detrimental to the District's network security as a whole. Secure substitutes for these services are generally available. For more information on how to obtain and use secure substitute for these services, please contact Network Security at (213) 241-1343.

2. Services Limited to LAUSD Headquarters

   There are network services necessary to maintain an Internet presence for the District that pose security threats if not properly managed and maintained. A list of examples may be found in Attachment B. Security of these services requires complex configuration and continuous analysis to verify their integrity. Due to the difficulty of maintaining these services, the District can only allow these services to be used within District headquarters for specialized purposes. These services will not be permitted to pass through the firewall to local sites.

3. Limited Services to Sites

   The District will continue to allow web servers or mail servers to be accessible through the District's firewall, provided the server is adequately secured. District personnel may request that additional services be granted through the firewall. As long as the requested services are not covered by 1or 2 above, requests will be reviewed on a case-by-case basis based on an assessment of the potential impact to the District's networks and the compelling need for access. In the event the District cannot allow a particular service through the firewall, the Network Security Office will work with the requesting party to evaluate acceptable alternatives.

B. Firewall Exception Request Procedure

There are cases where LAUSD personnel may believe it to be necessary, beneficial or convenient to allow access to servers located at a school or office from the public Internet. Staff or public Internet access to District servers through the firewall offers convenience but also compromises District security. The risk of creating additional access points through the firewall must be weighed against any need for access and the justification for such access must be compelling. Therefore, every request for staff or public Internet access to District servers through the firewall must be reviewed on a case-by-case basis to assess impact on network security.

This policy only applies to access to District servers via the Internet and access by District users to the Internet via District systems. This policy does not apply to access between servers, networks or users within LAUSD. For example, if a school or office establishes a web server to share information with other District sites and LAUSDNet dial-up users, the server does not require firewall access.

This policy does not apply to websites hosted on LAUSD's primary web server. Schools or offices within LAUSD may obtain space on LAUSD's primary web server to host Internet accessible content by emailing webmaster@lausd.k12.ca.us.

If District personnel wish to have a server accessible through the District's firewall, a "Firewall Exception Request" Form (Attachment A) must be completed and returned to ITD.

The certification signatures on the "Firewall Exception Request" permit the District to monitor the security of the server, and ensure the server administrator will not allow information the District deems sensitive to be stored on or transmitted from the server. The server administrator for the affected server is responsible for implementing appropriate security measures and access restrictions and is responsible for compliance with legal requirements regarding confidentiality and privacy.

Security of information of particular concern to the District includes the following:

- Information Protected by California Education Code and the Family Education Rights and Privacy Act (FERPA). This includes Children's Names, Children's images, descriptions, addresses, phone numbers, parent or guardian information, attendance, assessment information, transcripts, etc.
- Information Protected by the Health Insurance Portability and Accountability Act (HIPAA). This includes student health information, medical and personal history, federal program eligibility, disciplinary records, IEPs, special needs, etc.
- Information or services that are disallowed by the Children's Internet Protection Act (CIPA). This includes but is not limited to "visual depictions that are obscene or, with respect to the use of computers by minors, harmful to minors."
- Employee personal information.

Information of this type may not be made visible or accessible via the public Internet, with extremely limited exceptions. Student and Employee names and images may appear on District web servers, provided that each party depicted or, in the case of a minor, his or her parent or legal guardian has completed a release on a District approved form. The current District Release form may be downloaded from:

http://www.lausd.k12.ca.us/lausd/lausdnet/photo_release.pdf.

Information protected by Education Code, FERPA or HIPAA may be required to be shared with other agencies. In order for this information to be transmitted through the firewall, the requesting party must submit an information security plan along with the application. The information security plan must describe the following at a minimum:

- The encryption that will be deployed to protect the information during transmission.
- The authentication procedure that will ensure only trusted users have access to the information.
- The auditing procedure to monitor access to the information.
- An incident response plan that describes the steps that will be followed in the event of a security breach.

The information security plan will be submitted via ITD to the Office of the General Counsel for evaluation.

C. Firewall Exception Maintenance Procedure

Once an exception request has been approved, the Network Security Office will work with the requesting party's technical contact to verify the server operating system and applications. The District will then perform a preliminary security scan of the system. Once all security issues have been resolved, a firewall exception may be made.

The District reserves the right to scan periodically for configuration changes that may affect District security as a whole. The District may also require that software and applications be updated or reconfigured in a timely manner when new security vulnerabilities are discovered. Finally, the District requires that the server be maintained and kept in operational order, and that the site operators provide viable instructional and/or operational information. The District reserves the right to terminate server connections that are no longer providing reasonable service to the public or District personnel. If the server administrator is unable to comply with these procedures, the District may terminate the firewall exception. The District may also terminate the firewall exception if ITD can no longer contact the Administrator or the Technical Contact for the server. The contact information given to ITD must be current at all times. When the Technical Contact or Principal/Administrator changes, please complete a new form, note "Change of Contacts" on the top of the form and fax to (213) 241-8999.

# # #

LOS ANGELES UNIFIED SCHOOL DISTRICT
Information Technology Division

BULLETIN NO. K-24 (Rev.) ATTACHMENT A
November 4, 2002

DISTRICT WAN FIREWALL EXCEPTION REQUEST
CERTIFICATION

Please complete and return the following form. Return via school mail to the Information Technology Division Security Office, 10th Floor, Beaudry Building, or fax the completed form to (213) 241-8400.

CONTACT INFORMATION

Site Name: _______________ Location Code: _______________

FIREWALL DEFINITION REQUEST

Internal IP Address: _ _ _._ _ _._ _ _._ _ _ Requested Hostname: __________________

Service Requested: Web __ Secure Web __ Mail __ Secure Shell __

Other (Describe, including all required ports):
____
____
____

Reason for Request:
____
____
____

CERTIFICATION

I understand that a server at the above named site will be given access through the District's firewall to the public Internet. I therefore agree to the following conditions:

1. All District Policies, including the LAUSD Acceptable Use Policy (Bulletin K-19 rev.) and US Copyright laws will be observed.
2. The exempted server will not be used to store or transmit information that is legally protected by the California Education Code, the Federal Education Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the Children's Internet and Protection Act (CIPA). I understand that failure to comply with this requirement may result in disciplinary action, including termination.

3. The Information Technology Division (ITD) may periodically scan the exempted server for security vulnerabilities, and may require that changes be made to the server to repair detected vulnerabilities in a timely manner. I understand that ITD will provide notice via email to the technical contact prior to scanning.

4. In the event that the server is non-operational for an extended period of time, ITD will remove the exemption after providing notice to the technical contact via email.

I request exclusion from condition 2. An Information Security Plan is attached to this request for legal review. (Check here): _____

______________________________ Technical Contact (Please Print)	____________________________________ Principal/Administrator (Please Print)
______________________________ Employee Number	____________________________________ Employee Number
______________________________ Employee Phone Number	____________________________________ Employee Phone Number
______________________________ Email Address	____________________________________ Email Address
______________________________ Signature	____________________________________ Signature
______________________________ Date	____________________________________ Date

FOR OFFICE USE ONLY:

ITD Approval: ____________________________ Date: __________________________________

This attachment describes technical details of services that are allowed or disallowed from firewall exceptions.

The services described in this section are current as of the date of this document. New services and vulnerabilities are added on a continuous basis. A current list of disallowed services may be obtained from ITD Network Security by calling (213) 241-1343.

I. Disallowed Services:

Due to the high risk of the compromise of the District's WAN from intruders or the risk of illegal activity, the following services are explicitly denied through the District's firewall from points originating outside of the District:

Application	**Abbreviation**	**Port Number(s)**
AOL Instant Messenger	AIM	varies
AOL Client	(none)	5190
Directory Services	ldap	389
Finger	finger	79
Gnutella	none	6346, 6347
ICQ	ICQ	varies
Internet Relay Chat	IRC	6660-66670
Kazaa	none	1214
Mail Retrieval	POP, IMAP	109, 110, 143
MSN Messenger	msn	varies
Napster	none	varies
NetBIOS Services	netbios-ssn	135, 137, 138, 139
Network Time	time, ntp	37,123
NFS Services	portmap, rpcbind, NFS, etc.	111, 635, 2049, 4050
Open Windows	openwin	2000
PC Anywhere	(none)	5631, 5632
Small Services	varies	1-20
SNMP	SNMP	161
Sun Window Management	NeWS	144
System Log	syslog	514
Socks	SOCKS	1080
Terminal Services	rdp, icmp	3389, 1494
Terminal Link	link	87
Trivial File Transfer	tftp	69
Unix Remote Services	xec, rlogon, rshell, etc.	512-518
X Display Manager	xdmcp	177
X Windows	xwindows	6000-6255
Yahoo Messenger	(none)	varies

II. Services Limited to District Headquarters:

The following services are allowed through the District's firewall from points originating outside of the District to central servers managed by ITD:

Application	Abbreviation	Port Number(s)
Telnet	telnet	23
File Transfer Protocol	ftp	20, 21
Domain Name Service	DNS	53

III. Limited Services to Sites:

Schools or District offices ("sites") may request a server be made visible through the District firewall to the public Internet for the following services:

Application	Abbreviation	Port Number(s)
Web	http	80
Secure Socket Layer	https	443
Secure Shell	ssh	22
Mail	SMTP	25

In addition, schools may request individual ports that are not on this list be allowed on a case-by-case basis, provided they do not coincide with ports explicitly denied in I and II.