LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

TITLE: **Authorized Internet Service Provider (ISP) Connections To District Locations**

NUMBER: BUL-1759.0

DOCUMENT VISIBILITY ☐ PROTECTED ☒ PUBLIC

ISSUER: Megan Klee
Chief Information Officer
Information Technology Division

DATE: June 30, 2005

ROUTING
All Schools and Office

PURPOSE: This policy is to protect the District's computer network and information on the network from attack or unauthorized access. Only internet connections approved by Information Technology Division (ITD) can have access to the District network or District sites

MAJOR CHANGES: This is the first version of this document.

BACKGROUND: Over the past several years, District reliance on Information Systems designed to manage personal student and employee data has increased significantly. With this increased reliance has come a strong demand for access to District information and Internet resources from anywhere at any time.

At the same time, the threat of unauthorized access to personal data exposed via the Internet has also increased. Numerous recent additional laws and regulations have been enacted to increase the security of personal data, and government agencies have placed more stringent requirements on the manner the District may provide access to Internet resources.

In order to assure student and employee privacy and to comply with relevant privacy laws and Federal E-Rate requirements, the District has enacted policies intended to assure protection of confidential District information, including:

- Bulletin-999: Acceptable Use Policy (AUP) for District Computer Systems
- Bulletin-1077: "Information Protection Policy"
- Bulletin-1553: "Security Standards for Networked Computer Systems Housing Confidential Information"

It is every employee's obligation to comply with these Bulletins. These policies help ensure the District has appropriate privacy regulations and that the District is following current industry "best practices" for the protection of personal data. The District must secure all potential access points to sensitive information in a manner that assures both public confidence and regulatory compliance. The District network is designed to provide appropriate security only through Internet connections provided by ITD. The District does not have the resources to provide appropriate monitoring for alternative Internet connections. Therefore, specific written approval must be obtained from the Chief Information Officer for any connections to the Internet other than those provided through ITD.

Additionally, the Federal E-Rate program has placed stringent controls on how Internet access may be provided to students and staff. As a consequence, the District may not provide access to the Internet from dial-up connections offered to students and employees accessing the network from home. Students and staff who dial into the LAUSD network may access internal District resources (such as email and the District's website), and contracted Internet services such as e-Pals and resources from the Digital Library. The District may not allow access to the open Internet (such as Google and. Yahoo) via dial-up.

There are substantial risks/penalties to the District if unauthorized Internet connections are not closed in a timely manner. Examples include:

<u>The Integrated Student Information System (ISIS)</u>

- The ISIS application will be rolled out to all schools beginning after July 1, 2005. In accordance with industry standard security practices, the security of the system will require substantial monitoring of access to the system via the Internet. If a school or office sets up an alternative Internet Service Provider (ISP) or internal connection, the District will be unable to determine if malicious attempts to access the system from the internal network are actually from the Internet or a non-District location, and if so, the District will be unable to determine the primary point of attack.

<u>Compliance with the Children's Internet Protection Act (CIPA)</u>

- CIPA is a Federal Law stating the District must provide certain protections for children when accessing the Internet. These mandatory protections include the District filtering access to certain types of Internet sites. The District only has the ability to impose these protections on the ISP connections provided and managed by ITD. If a District school or office sets up alternative ISP connections not monitored for CIPA compliance by ITD, the District risks tens of millions of dollars annually in Federal programs requiring CIPA compliance as a condition for funding.

Compliance with Federal E-Rate Regulations

- The Schools and Libraries Division (SLD) of the FCC has stipulated that in order for the District to receive E-Rate funds, dial-up access to the Internet may not be provided. The SLD has also required the District to certify they are not providing this access in order to receive E-Rate funds for Internet connections in the next fiscal year.

Infrastructure Shortages

- Internet and/or District network connectivity frequently requires the use of permanent cabling from a school or office to public resources. The District has experienced issues in expanding the District connections necessary in some locations because infrastructure cabling was being used for unauthorized Internet connections.

These risks to the District are incurred regardless of the purpose of mechanism by which connectivity is being provided, regardless of the intended users or sponsors of the connectivity, and regardless of the perceived practicality of terminating the connection in a timely manner. This policy therefore applies to all current Internal and/or Internet connections, all District units and any connectivity type to the District's internal network and/or the Internet, including but not limited to:

- Leased Lines (T1, T3, OC3, ATM, etc.)
- DSL and or Cable Modems
- Cell phone-based Internet access
- Dial-up connections to internal District systems and/or the Internet
- Hardware-based Virtual Private Network (VPN) connections
- Software-based VPN Connections ("GotomyPC," Citrix, Microsoft VPN, etc.)
- Wireless technologies (i.e. 802 abg)

Specifically:

- All District locations including all schools, offices and work locations may connect to the Internet only through Internet Service Provider (ISP) Connections provided by the Information Technology Division (ITD) unless approved by the Chief Information Officer (CIO) on the attached form.
- All non-District locations used for instructional purposes by District staff and students (including but not limited to employee/student homes, business partner offices, independent charters who do not procure IT services from the District, and public facilities not owned or operated by the District) may connect to the District's internal network only through connections provided by ITD unless approved by the CIO on the attached form.

- All dial-up connections provided to employees, students and District business partners connecting to the District's internal network may access only resources owned and/or operated by the District or contracted District service providers.
- Any connection from a non-District location to the District's internal network and/or from a District location to the Internet via any connection not provided by ITD and not approved in writing by the CIO on the attached form must be terminated before August 1, 2005
- Any written or oral agreement between ITD and any District unit allowing any Internal or Internet connection not provided by ITD is considered void on July 1, 2005 unless specifically renewed on the attached form and authorized in writing by the CIO.

If any internal or Internet connection not authorized by this policy is discovered on or after August 1, 2005, ITD, on behalf of the District, may at its own discretion use any means at its disposal to permanently terminate the connection without warning to the users and/or to terminate the District location from all access to District systems until the unauthorized connection is terminated.

PROCEDURES: It is highly unlikely, but not inconceivable that a District unit may require access to the internal network from a non-District location or access to the Internet from a District location via a connection that cannot be provided by ITD and that the District would suffer a significant legal liability risk if an exception to the policy is not granted for this access. In these cases, an exception to this policy may be requested by using the attached form.

COMPLIANCE: (1) Violations of this policy may result in discipline, up to and including dismissal of personnel violating this policy

(2) Violations of this policy may also be violations of state and/or Federal law. Failure of personnel to comply with these policies could result in the employee(s) being sued for a violation of privacy rights, or being prosecuted by a governmental agency charged with enforcing those rights.

RELATED RESOURCES:

- Bulletin-999: Acceptable Use Policy (AUP) for District Computer Systems
- Bulletiin-1077: "Information Protection Policy"
- Bulletin 1553: "Security Standards for Networked Computer Systems Housing Confidential Information"
- Bulletin K-24: District Firewall Policy

ASSISTANCE: For further information, please contact Patrick Luce, Director of IT Security at (213) 241-1343.

Request for Approval for Non-ITD Provided Internet Service Provider Connection
FormITD-SEC-106
(Version 1,5/13/2004)

Los Angeles Unified School District
Information Technology Division

Identification (to be completed by the Administrator) Request Date: ____/____/____

Name (First) _____(MI) ____ (Last) _____

Title _____ Employee # _____

LAUSD email: _____@lausd._____

School/Office Name_____ Phone # ( ) _____ - _____

This document serves as a request for a network connection from the school or office shown above to the Internet via an alternative Internet Service Provider (ISP) to the Information Technology Division (ITD). Pertinent information regarding the requested ISP connection is provided below.

School or Office Location: _____Internet Service Provider Name: _____

Internet Connection type (T1/DSL/Cable Modem/etc.) _____

Purpose of connection:
_____
_____

Reason connection cannot be provided by ITD: (attach additional sheets if necessary)
_____
_____

Legal or Contractual requirements for ISP connection: (attach supporting documentation)
_____
_____

Signature of Requesting Administrator: _____

For ITD Use Only

Date Requested Received: ____/____/____

Security Recommendation: Approve/Deny Initials of ITD Security Director: _____

Chief Information Officer Decision: Approve/Deny

Signature of Chief Information Officer:_____ Date: ___/___/___

Please FAX this form to: Los Angeles Unified School District (Keep a copy)
(213) 241-8400