ROUTING
School Site Administrators
Central Office Administrators

TITLE: Description of Security Standards for Networked Computer Systems Housing Confidential Information

NUMBER: REFERENCE GUIDE NO. 3757.0

ISSUER: Charles A. Burbridge
Interim Chief Information Officer

DATE: June 13, 2007

BACKGROUND: The purpose of this Reference Guide is to describe minimum standards for the security of network-based security systems as described in Bulletin 1553.

GUIDELINES: Confidentiality is a property of information governing which individuals may access information and the required protection against unauthorized access. The mandate to protect information confidentiality comes from many sources. 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.

District information has varying requirements for confidentiality. Some information may be made widely available to the general public, while other information is subject to specific laws that govern who may view the information and under what conditions. To support these differing requirements for information protection, District information is categorized based on the confidentiality needs. Each category is then required to follow specific information protection practices. These practices include physical security, administrative practices, and technical configuration.

Confidentiality-based security controls may be distinguished from other security controls designed to enforce integrity and availability. Integrity is the property of data that allows it to be relied upon as an accurate representation of actual events. Integrity also involves

ensuring that data was properly entered by authorized individuals, and that the programs processing data operate in a known reliable way. Availability is the property of data that makes it available when required to support District business.

This reference guide emphasizes confidentiality-based security controls, though minimal mandatory baselines of integrity-based and availability-based controls are described. The minimum standards for confidentiality-based security controls of sensitive information described in this document are based on District Bulletin 1553.

DEFINITIONS

Data Owner: The executives or managers responsible for specific information that must be protected. The Data Owner has the final District responsibility of data protection. For instance, Financial Data would belong to the Chief Financial Officer, Human Resource data to the Personnel Commission or the Human Resources Department.

Business Owner: The administrator responsible for directing the operation of a computer or computer system and the applications residing on that system. Business Owners are those persons delegated the responsibility of protecting the information by the Data Owners. The Business Owner may or may not be the Data Owner of any data maintained on the system for which they are responsible.

Data Users: Individuals for whom the systems are designed. Data users may include students, parents/guardians, certified District employees, classified District employees, District vendors, and members of the public at large. Data users access system resources to achieve some benefit, in terms of their education, job duties, or citizen participation in District governance. Depending on the nature of the system, data users may or may not be individually identifiable.

Network-Based Computer System: A computer system used for storing data intended to be transmitted across District or non-District networks, where network access is an ongoing part of the system's use.

Stand Alone Computer System: A computer system used for storing data intended for personal use, not connected to any District internal network on a regular basis.

Security Plan: A document describing a system's security requirements and the measures required to ensure satisfaction of these requirements.

Physical Controls: Protections which prevent unauthorized physical access to devices containing or transmitting sensitive information. Physical controls prevent theft of devices or storage media, and unauthorized device reconfiguration through access to boot media, system consoles, or physical reset switches.

Technical Controls: Protections which prevent unauthorized access to sensitive information through configuration and management of technical resources such as servers, routers, and firewall devices. Technical controls cover management of user accounts and account privileges, access controls over data and programs, software configuration, and logical network service configuration.

Administrative Controls: Protections which prevent unauthorized access to sensitive information through encouraging individuals to follow policies, standards, guidelines, and procedures defining regular job activities and duties. Administrative controls cover the security goals for an organization and guidelines governing human use of computing resources.

Public Information: Information published on the District's public website or in other written District publications. Public Information is made available to the general public and may be accessed by any member of the public without prior authorization.

Non-Published Public Information: Public Information that exists in the form requested, but has not been published. For example, the District measures attendance on a daily basis. However, these daily attendance figures, while they are kept by the District, are not published. Non-Published Public Information requires the same security controls as Public Information. Non-

Published Public Information is made available to members of the public on request.

Non-Public Information: Information whose access must be guarded due to ethical, legal or privacy considerations. Non-Public Information is shared with internal parties on a "need to know" basis, and is not shared with external parties. Need to know is established by written permission of the data owner.

Protected Information: Information whose access is legally restricted to specific individuals. Protected Information generally requires a higher degree of confidentiality protection than Non-Public Information. Additional controls beyond those described in this document may be required depending on the specific legal requirements.

MINIMUM STANDARDS FOR SECURITY CONTROLS FOR NETWORK BASED COMPUTER SYSTEMS

Minimum standards are based upon the type of data as defined in Bulletin 1553. The Data Owner in consultation with the Director of IT Security and the Office of the General Counsel is responsible for determining the data sensitivity level. Once a sensitivity level has been defined, network-based computer systems housing that information must be approved by the data owner and must meet minimum standards for security controls as defined below. Any deviation from these standards must be reviewed for risk by the Director of IT Security and the Office of the General Counsel, and must be approved by the Data Owner(s). If the system is deemed by the Data Owner in conjunction with the Information Security Director and District Counsel to contain a particular threat due to scale of the information, the marketability of the information, or the potential for fraud or other misuse, additional controls beyond those specified below may be required at their discretion.

Minimum standards for each data sensitivity group are described in Table I in this document.

PUBLIC INFORMATION	NON-PUBLIC INFORMATION	PROTECTED INFORMATION
Definition	**Definition**	**Definition**
Public Information is information published on the District's public website or in other written District publications. Public Information requires no specific confidentiality protection; however Public Information requires security controls to protect data integrity and availability. Non-published Public Information is Public Information that exists in the form requested, but has not been published. For example, the District measures attendance on a daily basis. However, these daily attendance figures, while they are kept by the District, are not published. Non-Published Public Information requires the same security controls as Public Information.	Non-public Information is information whose access must be guarded due to ethical, legal or privacy considerations. Information that is confidential is shared with internal parties on a "need to know" basis, and is not shared with external parties. Need to know is established by written permission of the data owner.	Protected Information is information whose access is restricted to specific individuals by law. Protected Information generally requires a higher degree of confidentiality protection than Non-Public Information. Additional controls beyond those described in this document may be required depending on the specific legal requirements.
Examples	**Examples**	**Examples**
Examples include District data on overall enrollment, and other statistical or reference data available on the District's website.	Examples include employee addresses and home phone numbers.	Examples include student and employee health data protected by Federal Health Insurance Portability and Accountability Act (HIPAA) regulations, student information protected by Family Educational Rights and Privacy Act (FERPA), information relevant to investigations, information with attorney-client privilege, or information under a third party non-disclosure.
REQUIRED CONTROLS	**REQUIRED CONTROLS**	**REQUIRED CONTROLS**
Physical Controls – Equipment Housing	**Physical Controls – Equipment Housing**	**Physical Controls – Equipment Housing**

P-EH-1 Servers housing public information must be supervised during normal business hours	NP-EH-1 Servers housing public information must be supervised during normal business hours	PRO-EH-1 Servers housing public information must be supervised during normal business hours
P-EH-2 Servers must be kept in a locked room or cabinet	NP-EH-2 Servers must be kept in a locked room or cabinet	PRO-EH-2 Servers must be kept in a locked room or cabinet
		PRO-EH-3 Servers must be kept in a secured facility having specific physical protections defined by PRO-EH-3A through PRO-EH-3G
		PRO-EH-3A Individually assigned access codes must be maintained, so that all facility access is individually accountable
		PRO-EH-3B Hardcopy records must be kept of all facility access, listing the individual's identity, data and time of access and areas of the facility access
		PRO-EH-3C Visitors must sign in, and provide acceptable identification
		PRO-EH-3D Visitors who are not under contract with the District to perform specific tasks in the data facility must be accompanied by escorts
		PRO-EH-3E Intrusion alarms must be installed and must provide immediate response or data center facilities must be supervised 24 hours per day
		PRO-EH-3F Surveillance cameras must be installed. These cameras must be monitored by designated individuals or data center facilities must be supervised 24 hours per day
		PRO-EH-3G Environmental systems must include fire suppression, uninterruptible power supplies, temperature and humidity controls, emergency lighting, and smoke and fire alarms
Physical Controls – Backup Media Handling	**Physical Controls – Backup Media Handling**	**Physical Controls – Backup Media Handling**
P-BMH-1 Backup media stored on-site must be kept in a locked room or cabinet	NP-BMH-1 Backup media stored on-site must be kept in a locked room or cabinet	PRO-BMH-1 Backup media stored on-site must be kept in a locked room or cabinet

P-BMH-2 Backup media stored off-site must be kept only in locations authorized by the Data Owner and/or the Director of IT Security	NP-BMH-2 Backup media stored off-site must be kept only in locations authorized by the Data Owner and/or the Director of IT Security	PRO-BMH-2 Backup media stored off-site must be kept only in locations authorized by the Data Owner and/or the Director of IT Security
	NP-BMH-3 Backup media must be erased before disposal	PRO-BMH-3 Utilities approved by the Director of IT Security must be used to erase media prior to disposal
		PRO-BMH-4 When transporting data storage media off District premises, either all data must be encrypted using strong commercial encryption or an courier service approved by the Data Owner and/or the Director of IT Security must be used
Physical Controls – Storage Media Handling	**Physical Controls – Storage Media Handling**	**Physical Controls – Storage Media Handling**
n/a	NP-SMH-1 Computer hard drives must be reformatted before disposal, with a minimum of 1 pass of pseudorandom data overwriting each drive	PRO-SMH-1 Computer Hard drives must be physically removed and destroyed before disposing of obsolete systems
ADMINISTRATIVE CONTROLS - Operating System /Application Configuration and Maintenance	**ADMINISTRATIVE CONTROLS - Operating System /Application Configuration and Maintenance**	**ADMINISTRATIVE CONTROLS - Operating System /Application Configuration and Maintenance**
P-OSA-1 Servers and associated applications must be hardened on initial installation to security standards as provided by the Director of IT Security	NP-OSA-1 Servers and associated applications must be hardened on initial installation to security standards as provided by the Director of IT Security	PRO-OSA-1 Servers and associated applications must be hardened on initial installation to security standards as provided by the Director of IT Security and tested by the ITD Security Office.
P-OSA-2 Patches to the operating system and applications must be applied to fix critical security flaws before server implementation, or mitigating controls approved by the Director of IT Security must be applied for each known security issue resolved by unapplied patches.	NP-OSA-2 Patches to the operating system and applications must be applied to fix critical security flaws before server implementation or mitigating controls approved by the Director of IT Security must be applied for each known security issue resolved by unapplied patches.	PRO-OSA-2 Patches to the operating system and applications must be applied to fix critical security flaws before server implementation or mitigating controls approved by the Director of IT Security must be applied for each known security issue resolved by unapplied patches.

P-OSA-3 Operating System and application vendors must be consulted at least every 30 days to determine if new patches must be applied.	NP-OSA-3 Operating System and application vendors must be consulted at least every 30 days to determine if new patches must be applied.	PRO-OSA-3 Operating System and application vendors must be consulted at least every 30 days to determine if new patches must be applied
P-OSA-4 Patches pertaining to security flaws must be evaluated by the server administrator and the Director of IT Security for applicability. Patches deemed applicable must be applied in a timely manner as determined by the Director of IT Security	NP-OSA-4 Patches pertaining to security flaws must be evaluated by the server administrator and the Director of IT Security for applicability. Patches deemed applicable must be applied in a timely manner as determined by the Director of IT Security	PRO-OSA-4 Patches pertaining to security flaws must be evaluated by the server administrator and the Director of IT Security for applicability. Patches deemed applicable must be applied in a timely manner as determined by the Director of IT Security
P-OSA-5 Server configuration must be periodically reviewed by the Director of IT Security or designee for compliance with security standards	NP-OSA-5 Server configuration must be periodically reviewed by the Director of IT Security or designee for compliance with security standards	PRO-OSA-5 Server configuration must be periodically reviewed by the Director of IT Security or designee for compliance with security standards
	NP-OSA-6 Documented configuration control practices for operating system and application configuration must be approved by the Director of IT Security	PRO-OSA-6 Documented configuration control practices for operating system and application configuration must be approved by the Director of IT Security
		PRO-OSA-7 Server configuration must be periodically reviewed by an independent party for compliance with security standards
ADMINISTRATIVE CONTROLS - User Account Maintenance	**ADMINISTRATIVE CONTROLS - User Account Maintenance**	**ADMINISTRATIVE CONTROLS - User Account Maintenance**
P-UAM-1 Where Account Holders having individually assigned access exist, account provision must conform to the standards specified in requirements P-UAM-1A through 1D.	NP-UAM-1 Account provision must conform to the standards specified in requirements NP-UAM-1A through 1D.	PRO-UAM-1 . Account provision must conform to the standards specified in requirements PRO-UAM-1A through 1D.
P-UAM-1A Written management approval must be obtained prior to setting up individual user accounts	NP-UAM-1A Account Holders must have an individually assigned account for which they are responsible. Shared, group, or guest accounts must not be used	PRO-UAM-1A Account Holders must have an individually assigned account for which they are responsible. Shared, group, or guest accounts must not be used

P-UAM-1B System access must be removed immediately where the Account Holder has terminated their relationship with the District or changed locations within the District	NP-UAM-1B System access must be removed immediately where the Account Holder has terminated their relationship with the District or changed locations within the District	PRO-UAM-1B System access must be removed immediately where the Account Holder has terminated their relationship with the District or changed locations within the District
P-UAM-1C Account Holder access privileges must be assigned based on regular job duties	NP-UAM-1C Account Holder access privileges must be assigned based on regular job duties	PRO-UAM-1C Account Holder access privileges must be assigned based on regular job duties
P-UAM-1D Account Holder access privileges must be changed when job duties change. If a privilege is no longer required, it must be revoked	NP-UAM-1D Account Holder access privileges must be changed when job duties change. If a privilege is no longer required, it must be revoked	PRO-UAM-1D Account Holder access privileges must be changed when job duties change. If a privilege is no longer required, it must be revoked
ADMINISTRATIVE CONTROLS - User Account Training	**ADMINISTRATIVE CONTROLS - User Account Training**	**ADMINISTRATIVE CONTROLS - User Account Training**
P-UT-1 When user accounts exist, Account Holders must undergo basic security awareness training covering the District's Acceptable Use Policy and appropriate password management	NP-UT-1 Account holders must undergo security awareness training, emphasizing specific requirements for Non-Public Information management, handling of information downloaded from secure systems and security incident reporting in addition to the District Acceptable Use Policy and appropriate password management.	PRO-UT-1 Account Holders must undergo security training, covering desktop system security practices, Protected Information email practices, handling downloaded Protected Information, and other topics as determined by the Director of IT Security in addition to the District Acceptable Use Policy and password management
ADMINISTRATIVE CONTROLS - Confidentiality Assurance	**ADMINISTRATIVE CONTROLS - Confidentiality Assurance**	**ADMINISTRATIVE CONTROLS - Confidentiality Assurance**
N/A	NP-OV-1 Formal documented procedures for reporting and investigating confidential information breaches must be approved by the Director of IT Security and District General Counsel	PRO-CA-1 Formal documented procedures for reporting and investigating confidential information breaches must be approved by the Director of IT Security and District General Counsel
ADMINISTRATIVE CONTROLS - Verification of Outsourcing Practices	**ADMINISTRATIVE CONTROLS - Verification of Outsourcing Practices**	**ADMINISTRATIVE CONTROLS - Verification of Outsourcing Practices**

P-OV-1 Service provider (outsourcer) security practices must be evaluated by the Data Custodian for compliance with District standards for physical, administrative and technical controls.	NP-OV-1 Service provider (outsourcer) security practices must be evaluated by the Data Custodian for compliance with District standards for physical, administrative and technical controls.	PRO-OV-1 Service provider (outsourcer) security practices must be evaluated by the Data Custodian for compliance with District standards and with applicable regulatory requirements. Compliance criteria must be developed in consultation with District General Counsel and the Director of IT Security
TECHNICAL CONTROLS - Account Control	**TECHNICAL CONTROLS - Account Control**	**TECHNICAL CONTROLS - Account Control**
P-TAC-1 Where account holders having individually assigned access exist, they must conform to requirements P-TAC-1A through 1F.	NP-TAC-1 The system must be configured to prohibit any anonymous or unauthenticated access	PRO-TAC-1 The system must be configured to prohibit any anonymous or unauthenticated access
P-TAC-1A Non-trivial passwords must be enforced by technical measures. For example, in Windows 2000 an Account Policy may be defined to require minimum password length and password complexity requirements	NP-TAC-2 The system must be configured to enforce strong password selection for all user access via technical measures to meet requirements NP-TAC-2A through 2D.	PRO-TAC-2 The system must be configured to enforce strong password selection for all user access via technical measures to meet requirements PRO-TAC-2A through 2D.
P-TAC-1B Accounts must be disabled after 180 days of inactivity	NP-TAC-2A Passwords must be non-trivial	PRO-TAC-2A Passwords must be non-trivial
P-TAC-1C Accounts must be automatically disabled after 10 unsuccessful login attempts	NP-TAC-2B Passwords must be at least 8 characters in length	PRO-TAC-2B Passwords must be at least 8 characters in length
P-TAC-1D Password changes must be required at least every 365 days	NP-TAC-2C Passwords must consist of a mix of alphabetic and numeric characters	PRO-TAC-2C Passwords must consist of a mix of alphabetic and numeric characters
P-TAC-1E Account Holder access to files, commands, and application functions must be based on job requirements and enforced using system access control lists (ACLs). At a minimum, system software and application executables should provide write, update, and delete access only to Technical Administrators	NP-TAC-2D Passwords must not be a word found in a dictionary	PRO-TAC-2D Passwords must not be a word found in a dictionary

P-TAC-1F Only individually assigned system administrators may have privileged accounts, permitting operating system and security configuration	NP-TAC-3 Accounts must be disabled after 180 days of inactivity	PRO-TAC-3 Accounts must be disabled after 180 days inactivity
	NP-TAC-4 Accounts must be automatically disabled after 5 unsuccessful login attempts	PRO-TAC-4 Accounts must be automatically disabled after 5 unsuccessful login attempts
	NP-TAC-5 Password changes must be required at least every 180 days	PRO-TAC-5 Password changes must be required at least every 180 days. The system shall be configured to disallow reusing passwords successively.
	NP-TAC-6 Account Holder access to files, commands, and application functions must be based on job requirements and enforced using system permissions or access control lists (ACLs).	PRO-TAC-6 Application access must time out after an idle time of 30 minutes. This timeout must be independent of any workstation or network access timeout.
	NP-TAC-7 Default read access to confidential data must be set to none" via system permissions or ACLs	PRO-TAC-7 Account Holder access to files, commands, and application functions must be based on job requirements and enforced using system permissions or access control lists (ACLs).
	NP-TAC-8 Only individually assigned system administrators may have privileged accounts, permitting operating system and security configuration	PRO-TAC-8 Default read access to confidential data must be set to none" via system permissions or ACLs
		PRO-TAC-9 Only individually assigned system administrators may have privileged accounts, permitting operating system and security configuration
		PRO-TAC-10 If feasible, end users should be restricted to only a single application session, to discourage sharing IDs and passwords.

		PRO-TAC-11 If feasible, at time of application login, the date and time of the end user's last access must appear. End users must be trained to review this information and to report any discrepancy between the displayed date and time and the user's recollection of their last access
TECHNICAL CONTROLS - AntivirusControl	**TECHNICAL CONTROLS - AntivirusControl**	**TECHNICAL CONTROLS - AntivirusControl**
P-AV-1 All servers must be configured to automatically run appropriate anti-virus software as required by the Director of IT Security	NP-AV-1 All servers must be configured to automatically run appropriate anti-virus software as required by the Director of IT Security	PRO-AV-1 All servers must be configured to automatically run appropriate anti-virus software as required by the Director of IT Security
P-AV-2 Where anti-virus software is applied, anti-virus signatures automatically must be checked for update on a daily basis, with signatures updated immediately upon availability	NP-AV-2 Where anti-virus software is applied, anti-virus signatures automatically must be checked for update on a daily basis, with signatures updated immediately upon availability	PRO-AV-2 Where anti-virus software is applied, anti-virus signatures automatically must be checked for update on a daily basis, with signatures updated immediately upon availability
TECHNICAL CONTROLS - Event Logging	**TECHNICAL CONTROLS - Event Logging**	**TECHNICAL CONTROLS - Event Logging**
P-EL-1 Servers must be configured to log the following events defined in P-EL-1A through 1C locally:	NP-EL-1 Servers must be configured to log the following events defined in NP-EL-1A through 1C locally:	PRO-EL-1 Servers must be configured to log the following events defined in PRO-EL-1A through 1C locally:
P-EL-1A Changes to the server's security policy	NP-EL-1A Changes to the server's security policy	PRO-EL-1A Changes to the server's security policy
P-EL-1B Successful and unsuccessful authentication attempts, if authentication is enabled	NP-EL-1B Successful and unsuccessful authentication attempts	PRO-EL-1B Successful and unsuccessful authentication attempts
P-EL-1C Privileged access to system resources.	NP-EL-1C Privileged access to system resources.	PRO-EL-1C Privileged access to system resources.
P-EL-2 Event logs must be reviewed by the Data Custodian or a designee on a weekly basis for high-risk events.	NP-EL-1D Unsuccessful attempts to access files, execute programs, or perform other actions blocked by security rules	PRO-EL-1D Unsuccessful attempts to access files, execute programs, or perform other actions blocked by security rules
	NP-EL-2 Event logs must be reviewed by the Data Custodian or a designee on a daily basis for high-risk events.	PRO-EL-2 Event logs must be reviewed by the Data Custodian or a designee on a daily basis for high-risk events.

		PRO-EL-3 Servers must log Additional event types, as required by regulation or policy governing the Protected Information.
		PRO-EL-4 Event logs must be recorded both locally on the server itself and remotely on a log server designated by the Director of IT Security. Logs must be retained for a minimum of 90 days, unless longer retention is required by regulation.
TECHNICAL CONTROLS - Encryption	**TECHNICAL CONTROLS – Encryption**	**TECHNICAL CONTROLS – Encryption**
P-ENC-1 When individual access is employed, both the password prompt and the password sent back to the server must be encrypted across all networks, both LAUSD-controlled and outside networks.	NP-ENC-1 All Non-Public Information traversing non-LAUSD networks must be encrypted	PRO-ENC-1 All Protected Information traversing between client computers and web or application servers must be encrypted between source and destination using the strongest commercially available encryption as determined by the Director of IT Security
	NP-ENC-2 Password prompt and the password sent back to the server must be encrypted across all networks, both LAUSD-controlled and outside networks	PRO-ENC-2 Privileged access must use an encrypted Virtual Private Network (VPN) or equivalently strong mechanism approved by the Director of IT Security for both local network and Internet access
	NP-ENC-3 Where encryption is used, the strongest available commercial encryption as determined by the Director of IT Security must be configured	PRO-ENC-3 All user account passwords must be stored in encrypted form on the local system.
TECHNICAL CONTROLS - Traffic Filtering	**TECHNICAL CONTROLS - Traffic Filtering**	**TECHNICAL CONTROLS - Traffic Filtering**
N/A	NP-TF-1 The primary data repository for Non-Public Information must not reside on a publicly accessible Web server. If non-public information is accessible from non-District networks, data must reside on a separate server located within a firewall DMZ specifically assigned to Non-Public Information database servers.	PRO-TF-1 The primary data repository for Protected Information must not reside on a publicly accessible Web server. If non-public information is accessible from non-District networks, data must reside on a separate server located within a firewall DMZ specifically assigned to Non-Public Information database servers.

	NP-TF-2 Servers housing Non-Public Information must implement host-based TCP/IP filtering to restrict access to authorized services. TCP/IP filtering or IPSec filtering may be used for Windows 2000 servers, ipfw or ipchains for Linux servers or Apple servers, or other equivalent products as applicable.	PRO-TF-2 Servers housing Protected Information must implement host-based TCP/IP filtering to restrict access to authorized services. TCP/IP filtering or IPSec filtering may be used for Windows 2000 servers, ipfw or ipchains for Linux servers or Apple servers, or other equivalent products as applicable.
		PRO-TF-3 Network traffic containing Protected Information must separated from other District traffic by assigning specific IP subnets, use of a Virtual LAN (VLAN) or other measure approved by the Director of IT Security.
TECHNICAL CONTROLS - Intrusion Detection	**TECHNICAL CONTROLS - Intrusion Detection**	**TECHNICAL CONTROLS - Intrusion Detection**
N/A	N/A	PRO-ID-1 File integrity validation must be used on servers to determine if critical files have undergone unauthorized modification.
		PRO-ID-2 Host intrusion detection systems must be installed on servers hosting Protected Information, or equivalent or mitigating controls approved by the Director of IT Security must be used.

ASSISTANCE: For further information, please contact Gash Teshome, IT Security Coordinator at (213) 241-0627.