CHARLESTON COUNTY SCHOOL DISTRICT

Department of Information Technology

Information Technology Security Standards

Issued August 7, 2006

Introduction

These security standards apply to users of Charleston County School District (CCSD) information technology. Users include students, employees and other individuals having access to CCSD technology. The standards apply to contractors with respect to technology services they supply to CCSD, such as processing of student or employee data for CCSD.

The standards are authorized by Policy GBEBD, Technology Acceptable Use, adopted by the Board of Trustees January 9, 2006.

In these standards, the term 'nonpublic' means not disclosable under applicable federal, state, or local law or regulation. Examples are students' date of birth, grades, personal medical information, and CCSD attorney-client privileged information.

The term 'essential information ' means information which if lost or corrupted may disrupt operations essential to provision of CCSD services. Examples are computer system passwords, CCSD bank account numbers, social security numbers, and employee emergency contact information.

1. Access Controls

a. User Authentication

User IDs – User IDs are required to access any nonpublic or essential information. User IDs may consist of the user name, e-mail name or other public identifier. Generic User IDs, such as 'student_user', which may be utilized by multiple persons, should be avoided whenever possible, and are never to be used to access nonpublic or essential information.

Passwords – Special rules apply to passwords. These are provided in Appendix A, Password Standards.

b. User Authorization

User authorization – the creation of a user account - is to be granted by the system owner or administrator. Authorization is to be limited to the period for which access is required. Student user access is authorized for the duration of enrollment in CCSD schools, and is to be terminated thereafter. Student authorization is limited to each specific individual, and is not to be shared with

adults or other students. User authorization is to be canceled immediately upon termination of an employee or expulsion of a student. User rights are to be established only for the system functions required by an individual user. User sessions should time out or terminate after a designated period of inactivity.

c. System Access

Network access – Network access requires user authentication and authorization conforming to the standards above. Access to the network through the login process requires the user to acknowledge and accept Terms of Use, which include compliance with the CCSD Technology Acceptable Use policy (Policy GBEBD).

Remote access – Virtual private network (VPN) access may be granted by approval of the Information Technology Department. Dial-in and telnet access are not permitted directly into the CCSD network or systems.

Wireless access – Wireless end user devices must be protected from intrusion, for example by firewall software installed on the device and properly configured for safe internet access. Passwords, nonpublic or essential information transmitted over wireless sessions must be encrypted to meet current cryptographic requirements established by Information Technology.

User authorization will be required to access CCSD wireless networks. Only access points approved by Information Technology may be attached to the CCSD network. New CCSD wireless access points must be configured for cryptographic protection equal to or better than WPA2 standards.

Filtering, Monitoring, and Disclosure of Communications – Data communications to or from the Internet must be screened by CCSD filtering, firewall and intrusion detection systems. Communications including e-mail and web content are filtered for viruses, embedded malicious software, and known sources of spam or hackers. Communications are also filtered for content which may be inappropriate or may violate standards of the Children's Internet Protection Act or the CCSD Technology Acceptable Use policy (Policy GBEBD). CCSD electronic communications may be monitored, disclosed, used for disciplinary action, or reported to law enforcement authorities**. Users of CCSD information technology are advised that they have no expectation of privacy in use of CCSD electronic communications.**

Firewall and Intrusion Protection – The Information Technology department determines services and ports that are available at the firewall. Some ports and services in common use are not available for third party systems or vendor use due to security requirements. Intrusion attempts are monitored and may be subject to disclosure, disciplinary or legal action.

Audit logs – System actions on the CCSD network such as access attempts, login sessions, security violations, and other events are logged and monitored by CCSD. All applications and servers used by CCSD, whether operated by CCSD or by third parties, are to maintain audit logs of all security related events. The system administrator for such applications or servers is required to monitor audit

logs and report promptly any violations of these Security Standards or repeated attempts at violations to CCSD Information Technology.

2. Physical security

Servers and network equipment - Access points and network devices which are mounted in public areas shall be inaccessible without ladders or special equipment whenever possible. Servers and network equipment are to be protected from public access. Servers and network devices processing nonpublic or essential CCSD information shall be in locked spaces with access limited to authorized individuals. Telecommunications rooms shall not be used for storage of office or janitorial supplies or other non-IT equipment. Power conditioning, automatic fire suppression, and proper HVAC shall be provided to all such equipment spaces.

Workstations and printers – Workstations and printers used to access nonpublic or essential information shall be protected from public access, and display or printing of the information shall be protected from view by unauthorized persons. Workstations storing such information shall be properly secured when not in use. Backups of these systems shall be made as frequently as necessary to protect against data loss, and the backups kept in a separate, secure location. Backup to servers is an acceptable method.

Laptops and other portable devices – Portable devices such as laptops, PDAs or tablets must be carefully protected from theft or accidental damage. In addition the equipment should be used or transported in an environment for which it was designed. When nonpublic or essential information is stored on a portable device, a copy of the data should be maintained on a fixed platform such as a server, to protect against data loss.

Backups of these systems shall be made regularly and as frequently as necessary to protect against data loss, and the backups kept in a separate, secure location. Access to portable devices containing such data must be controlled by user authentication to prevent intrusion. Anti-virus software is to be maintained on all portable computers, and the systems scanned regularly.

Media – CDs, DVDs, and USB flash drives are convenient but highly vulnerable to theft or loss. They are also common carriers of viruses and malicious software that can disrupt an otherwise secure network. Therefore these media require special care. They are never to be shared with unauthorized persons. In the event portable media are used with both CCSD and non-CCSD systems such as home or business computers, all files on the media must be thoroughly scanned for viruses and malicious software before use on a CCSD system.

Disposal of devices containing CCSD software and/or data – PC hard drives, USB flash drives, backup tapes, diskettes, CDs and DVDs containing CCSD data are to be physically disabled or destroyed prior to disposal. Deleting files or running disk-wipe software are insufficient to protect CCSD data from being recovered by unauthorized persons and misused.

3. Data Security

Data display – Nonpublic data shall not be displayed to the public, nor shall passwords or other essential system information be posted or visible to unauthorized persons.

Data storage and transmission – Nonpublic and essential information shall be encrypted prior to and during storage, and during transmission over the internet, using encryption meeting current cryptographic requirements established by Information Technology. Passwords, e-mail, and FTP file transfers containing nonpublic or essential information, shall be encrypted during transmission.

Content Filtering – Data, including e-mail, files and web content entering the CCSD network, shall be filtered in a manner to meet the standards of the federal Children's Online Protection Act.

Backup and recovery requirements – A backup schedule shall be created and maintained by the person responsible for each server. Backups to tape or other removable media shall not overwrite the immediately preceding backup. Removable backups shall be labeled as to the most recent batch, and kept in a separate, secure location. Frequency of backups shall be appropriate to the value of the contents, generally daily for servers.

4. Application Security

New software applications developed for CCSD shall be designed and developed to conform to these standards. Security for existing software applications, including commercial off-the-shelf-software, shall be configured to conform to these standards by the system administrator or integrator. Implementation of applications shall include change of default passwords provided with the product.

5. Non-CCSD Hardware and Software

Non-CCSD hardware and software shall not be connected to the CCSD network unless specific written authorization has been granted by Information Technology. DSL and cable modems may not be connected to the network. Any non-CCSD hardware or software which is authorized for connection to the CCSD network shall be used in conformance with these security standards.

6. Incident Reporting

Security incidents and violations of these standards shall be reported promptly to the Executive Director of Information Technology or designee**.**

7. Security Requirements for Consultants, Contractors and other Non-CCSD Personnel

CCSD data accessed by contractors or other persons shall be handled in compliance with these security standards. Personnel employed by contractors or their subcontractors shall have proper qualifications and credentials for any access they have to nonpublic or essential CCSD data.

8. Administration by the Department of Information Technology

The Department of Information Technology shall administer these standards. It shall update them when needed, and prescribe non-user technical security measures required for information systems, including devices not specifically covered in these standards such as network switches, routers, and system software.

9. Standards not Exclusive

These standards are in addition to any other security standards required by applicable law, regulation, contract, or license, and where any conflict may arise between these and other required standards, the higher standards shall apply.

10. Enforcement

Enforcement of these standards shall be carried out under the provisions of Policy GBEBD.

APPENDIX A

CHARLESTON COUNTY SCHOOL DISTRICT
Department of Information Technology

Password Standards for System Users

1. The initial password provided to a system user must be changed by the user immediately upon gaining access to the system for the first time.

2. The password must be different from the User ID.

3. The password must not contain any part of the user's name or social security number.

4. The password must be non-intuitive. For example the name of a pet or family member, home address, or other readily discoverable term must not be used.

5. Passwords must consist of a minimum of six mixed alphabetic and numeric characters. They may not consist solely of numbers, or alphabetic, or special characters. Also, they must contain not more than two consecutive identical characters, and should not contain leading or trailing blanks.

6. Passwords should be changed at least every 90 days. Network passwords for student network accounts have longer durations based on grade levels.

7. A changed password must differ substantially from the old password. More than one character must be changed. Old passwords must never be re-used.

8. Default passwords on CCSD equipment including network electronics must be changed after first use.

9. Passwords are confidential. They are never to be shared or displayed.

10. The 'Remember password' feature of applications must not to be used.

11. If a password is forgotten or lost, contact the system administrator or school employee designated to reset passwords. System administrators cannot see or determine a user's password, and should never require that it be disclosed to them. They can generally cancel a lost password and issue a new one-time password which must be changed by the user immediately upon regaining system access.

rev. July 31, 2006