INFORMATION TECHNOLOGY

Technology Infrastructure

FCPS Information Security Policy

This regulation supersedes Regulation 6225.5.

I. PURPOSE

To establish computer data security policies for Fairfax County Public Schools’ (FCPS) computer systems and network resources.

II. SUMMARY OF CHANGES SINCE LAST PUBLICATION

A. In section IV., CIO has been changed to Assistant Superintendent of Information Technology.

B. In section V., language regarding application security standard and FCPS Security Profile has been added. Also, under Incident Handling, “Office of Equity and Compliance” has been changed to “Office of Equity and Employee Relations,” and “Department of Communications and Community Outreach” has been changed to “Office of Communications and Community Relations.”

III. SCOPE

A. Definitions

Audit: To conduct an independent review and examination of network or system policies, configurations, records, and activities.

Computer Security Incident: A violation, or imminent threat of violation, of computer security policies, or acceptable use policies or a disruption of network operations.

Computer System(s): Includes, but is not limited to, all the following terms used in the FCPS computer network: hardware, software, data, communications devices, terminals, printers, micro, mini, and mainframe computers, personal digital assistant (PDA) devices, smart phones and tablets.

Data Custodian: Person or team designated by the data owner to be responsible for managing the data in order to maintain its confidentiality, integrity, and availability.

Data Owner: Designated member of the FCPS management team who is authorized to grant or deny access to data and who is ultimately responsible for the confidentiality,
integrity, and availability of the data. A data owner can be, and often is, the system owner or sponsor.

Encryption: Algorithmic process used to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Firewall: A collection of components or a system that is placed between two networks and possesses the following properties: 1) all traffic from inside to outside, and vice versa, must pass through it; 2) only authorized traffic, as defined by the security policy is allowed to pass through it; 3) the system itself is immune to penetration by general standards.

Mobile Device: Also known as a “handheld device,” is a small computing device that has an operating system and can run various application software.

Need to Know: Also known as “least privilege,” the principle that requires each subject be granted the most restrictive set of privileges needed to perform authorized tasks. The application of this principle limits the damage that can result from an accident, error, or unauthorized use.

Passphrase: A sentence or phrase used as a password. Its longer length makes it harder to break, and using a sentence or a phrase makes it easier to remember.

System Custodian or Administrator: The individual or group that is designated by the system sponsor to handle the administrative tasks of managing and maintaining the system.

System Sponsor or Owner: The individual, director level or above, responsible for initiating procurement and granting access to, and defining requirements for, the system.

Users: All individuals who have access to FCPS computing resources.

Virtual Private Network (VPN): A method for accessing a remote private network via "tunneling" through the Internet. Data is typically encrypted when traveling through the VPN tunnel.

B. Applicability

This regulation applies to all computer systems and all network users in FCPS.

IV. Ownership and Responsibility

School Board and the Leadership Team
The School Board, Superintendent, and Leadership Team of FCPS have the ultimate responsibility to fulfill due-care and due-diligence requirements regarding information security. They ensure that the division-wide information security program is implemented, effective, and well supported by resources.
Assistant Superintendent of Information Technology
The Assistant Superintendent of Information Technology is responsible for the planning, budgeting, and performance of data security components. The Assistant Superintendent of Information Technology shall direct the development and implementation of the information system security program, assign roles, delegate responsibilities, and advise the School Board and Leadership Team members on information security.

System and Data Sponsor or Owner
Sponsors are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of systems and information. Sponsors initiate the procurement process, designate the information classification, grant access rights to user groups, and ensure compliance with applicable laws, regulations, policies, and standards. All systems and data have clearly designated sponsors. Principals and program managers are typically sponsors or owners for the respective systems and information in their custody.

System and Data Custodian or Administrator
System and data custodians are responsible for the proper implementation of security requirements. System administrators, technical support specialists, school-based technical specialists, and functional application support teams are custodians of the systems and information for which they are responsible. When systems and information are maintained on a personal computer, the user is the information custodian. Custodians should be in constant communication with sponsors or owners to keep systems up and running securely, thus ensuring the long-term health of the systems and information.

V. Information Security Standards

Acceptable Use
Regulation 6410 defines the acceptable use policy for all FCPS users.

Account Management
The system sponsor is the owner of the accounts on his or her system and is responsible for identifying individuals who have access to the system, determining the level of access an individual shall have, and designating a custodian of the accounts.

The IT Service Desk is the custodian of the network user accounts and is responsible for the creation, modification, and deletion of the accounts. Each user is responsible for safeguarding his or her accounts and preventing it from being misused. The user shall never allow others to use his or her accounts. Users who use FCPS computing resources should review and follow this regulation and the FCPS information security guidelines (see section VI.).

The employee account shall uniquely identify each user. The need-to-know principle shall be used to assign access rights to user accounts. Upon change or loss of a need to know, user accounts shall be promptly modified or removed. Accounts should be audited periodically.
Application Standard
Enterprise applications should adhere to the standard set forth by the FCPS Security Profile (http://fcpsnet.fcps.edu/it/offices/ito/nss/data_security/FCPS%20Security%20Profile%2020131029.htm). This link is available only through computers within the internal FCPS network (FCPSnet).

Audit
Information security policies, procedures, and practices shall be subject to periodic audit by FCPS personnel or independent auditors. If the audit involves a third party network, written approval must be obtained from the third party prior to the audit.

Backup
Backup shall be performed for all mission-critical systems on the FCPS network. Backup frequencies, methods, and retention times are determined by the system sponsor based on the business needs and requirements of the regulations.

Critical System Change Management
Changes, both scheduled and unscheduled, to mission-critical systems and their computing environment facility shall follow the change management process.

Data Classification
Each data owner must determine the classification(s) of the data he or she owns and must ensure that the data custodian is protecting the data appropriately. Data custodians are responsible for implementing data protection policies and procedures. Restricted and private data must be protected to the degree appropriate to their security level. FCPS data are classified in the following three security levels:

1. Public Data—Information to which the general public may or must be granted access, according to the Virginia Freedom of Information Act (VFOIA) and other applicable statutes.

2. Restricted Data—Information that shall be guarded due to proprietary, ethical, or privacy considerations, is exempt from release under VFOIA, and shall be protected from unauthorized access, modification, transmission, storage, or other use. Members of the FCPS community may be granted access to restricted data. Disclosure of restricted data to people outside FCPS may be granted based on business or educational need to know or as required by law, policy, or legal process.

3. Private or Sensitive Data—Information protected by statute, regulation, FCPS policy, or contractual language, and personal information about an individual that the individual can reasonably expect will not be made available to the public. Mishandling of private information may affect FCPS through financial and legal sanctions, loss of public confidence, and damage to FCPS’ reputation. Access to private data shall be granted on a need-to-know basis only in accordance with statute, regulation, policy, and contractual language.
Disaster Recovery (DR) and Business Continuity Planning (BCP)
Department of Information Technology, Information Technology Operations, is responsible for developing, maintaining, and implementing a disaster recovery and business continuity plan for the Network Operating Center (NOC) to minimize the potential impact of an unexpected event. System sponsors and owners are responsible for developing DR and BCP for systems outside the NOC.

File Storage
It is strongly recommended that files containing sensitive information be saved to a network drive. If these files have to be saved to the local drives of a desktop or a laptop computer, or to a mobile storage device including, but not limited to, a flash drive or a CD, they must be encrypted.

Firewall
Department of Information Technology, Network and Systems Services (IT NSS), is the system owner and custodian of all firewalls on the FCPS network. All Internet-facing gateway access points must be protected by a firewall. Access from external networks must be approved by IT. Any such access, if granted, should be as restrictive as possible. External-facing services that require open ports on the firewall must meet security requirements and be registered with and approved by IT NSS.

Incident Handling
Personnel-related incidents that require investigation shall be directed to the human resources investigator or the director of the Office of Equity and Employee Relations in the Department of Human Resources. Student-related incidents shall be referred to the school administration. IT shall provide technical assistance to the investigations.

IT is responsible for investigating interruptions to network and system operations and shall be notified immediately of any compromise to passwords or data.

Should an incident reach media attention, all requests for information should be directed to the Office of Communications and Community Relations.

Internet Filtering
Internet filtering is mandated by the Children’s Internet Protection Act. All computers in Fairfax County schools and administrative centers must be filtered. FCPS curriculum committee decides which categories to block in reference to Virginia Code. Each school can customize the policy and add sites to the blocked list.

Media Disposal
Data on the hard drives shall be destroyed before the computer leaves FCPS premises. Soft media, including but not limited to CD, DVD, floppy diskette, JAZZ drives, ZIP drives, and memory stick, shall be destroyed when the media is disposed.

Mobile Devices
A pass code must be configured for mobile devices used to download or store FCPS sensitive information.
Network Infrastructure
IT NSS is the owner and custodian of all network infrastructure devices in the FCPS network, including but not limited to routers, switches, hubs, firewalls, VPN concentrators, and wireless access points. All network cables and network devices must be installed by IT NSS or an FCPS-approved contractor with the consent of IT NSS. Unauthorized access to network devices is prohibited. Configuration of the network devices shall conform to the configuration standards set forth by IT NSS. IT reserves the right to monitor all traffic on the FCPS network and to disconnect devices that interrupt network operations.

Passwords
FCPS users are responsible for the security of their passwords and must not reveal passwords to others. FCPS support staff members will not ask a user for his or her password. Users are prohibited from using any password or account other than their own. Users should always logoff or lock their computers when stepping away from their desks. Never leave a terminal unattended and open.

Passwords should be changed annually and more often if required by the system sponsor. An employee’s, contractor’s, or a middle or high school student’s password must be at least eight (8) characters long and must contain at least one (1) uppercase alphabetic character, one (1) lowercase alphabetic character, and one (1) numeral. Passwords shall not be a user’s initials, proper names, license plate numbers, birth dates, social security numbers, etc., or any other character strings with characteristics that may identify the user.

Physical Security
All computing resources must be physically protected in relation to their value to FCPS and must comply with all applicable regulations, including but not limited to building and fire codes.

Mission-critical systems should be stored in a location that protects them from unauthorized physical access. Measures (locks, badges, keycard, etc.) shall be implemented to restrict the access to the systems.

Remote Access
Remote access shall be provided to FCPS users on the basis of business need and shall be used for mission-related purposes. Remote users must be compliant with FCPS policies and regulations.

Remote access connection should be given the same consideration as the user’s on-site connection to FCPS. Personal equipment that is used to connect to the FCPS network must meet the requirements of FCPS-owned equipment.

Security Awareness and Training Program
All users that access FCPS network resources shall accept the FCPS acceptable use policy, and receive security awareness training. IT, in coordination with principals and program managers, shall develop a security awareness and training program. System sponsors shall ensure that staff members receive security training to understand the security requirements of the information.
Server Security
Each server on the FCPS network shall have its own designated sponsor who is responsible for the overall security of the server and for designating a system administrator for everyday operations. All servers on the FCPS network should be registered with IT NSS. System administrators shall establish, document, and implement configuration standards that are compliant with FCPS policies and standards.

Use of Privately Owned Equipment
As a general rule, only FCPS equipment is allowed on the FCPS network. However, to provide convenience to FCPS users, privately owned equipment is allowed if it meets all the following standards:

1. Users are FCPS students, faculty, staff members, or authorized vendors.
2. The use is mission related.
3. The use is approved by the principal or program manager.

All FCPS regulations and computer use policies apply to the privately owned equipment.

FCPS is not responsible for any loss or damage to privately owned equipment, software, or data. School-based technical resources may be used, subject to approval of the principal or program manager, to help people using privately owned equipment on the FCPS network. Central resources shall not support the use of privately owned equipment.

Employees should be aware of the risks of connecting a personal smart phone device (such as iPhone or Droid) to the FCPS network. These risks include the complete loss of all data on the device. It is strongly recommended that only FCPS-issued devices be configured to download FCPS e-mail.

Virus Protection
All servers and workstations connected to the FCPS network must use a virus protection program approved by IT. Users should not disable virus protection at any time. Exceptions can only be granted on temporary bases and must be approved by IT.

System administrators shall develop plans to keep security patches and the antivirus programs up-to-date on the servers and workstations if applicable. E-mail messages and their attachments must be scanned for viruses when coming to the e-mail server.

E-mail found with viruses or suspicious files shall be removed from the delivery system. Any device found with a virus must be taken off the network immediately and be cleaned and verified virus free. Systems that cannot be cleaned shall be reimaged. IT has the discretion to block network traffic suspicious of carrying any form of virus.

Wireless
IT NSS is the custodian of all approved wireless access points and is responsible for establishing procedures and standards on wireless implementation and maintenance. Only approved equipment and technology can be purchased and installed on the FCPS network. Rogue (unauthorized) access points are prohibited.
Configurations of the access point (AP) must adhere to the standard set forth by IT. IT will only maintain approved APs and reserves the right to disconnect any AP that interrupts normal network operation. Sensitive information, including but not limited to student records, must be transmitted over an encrypted and authenticated wireless network.

VI. INFORMATION SECURITY GUIDELINES

The FCPS information security guidelines section outlines the fundamental security principles that FCPS shall follow in its handling of critical electronic information. Please refer to the guidelines (http://fcpsnet.fcps.edu/it/offices/ito/nss/data_security/guidelines_fcps.shtml) for more details on FCPS information security policies. This link is available only through computers within the FCPS network (FCPSnet).

Also see the current version of: Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources.