Regulation 6226.1
Information Technology
Information Technology
Operations
Effective 5/21/19

INFORMATION TECHNOLOGY

Technology Infrastructure

Fairfax County Public Schools (FCPS) Payment Card Industry (PCI) Security Policy

This regulation supersedes Regulation 6226.

I. PURPOSE

To establish computer data security policies for Fairfax County Public School (FCPS) personnel, computer systems, and network resources that process payment card information.

This regulation applies to all computer systems and resources, as well as all network users in FCPS that process payment card information. This regulation shall supersede Regulation 6225, FCPS Information Security Policy, in its applicable scope whenever discrepancies arise.

II. SUMMARY OF CHANGES

Added the following requirements in accordance with PCI Security Standards:

A. Section III.J. - Dual factor authentication shall be employed for accounts used in cardholder data environment.

B. Sections V.A. and V.P. - Default credential must be changed prior to deployment.

III. DEFINITIONS

For the purpose of administering this regulation, the following terms are defined:

A. **Audit** - To conduct an independent review and examination of a network's and/or system's policies, configurations, records, and activities.

B. **Authentication Factor** - A category of credentials that is intended to verify a user's identity.

C. **Business Continuity Plan (BCP)** – A BCP describes the process and procedure an organization puts in place to ensure that essential functions can continue during and after a disaster. BCP seeks to prevent interruption of mission-critical services and to reestablish full functionality as swiftly and smoothly as possible.

D. **Cardholder Data Environment** – "Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission." (PCI Security Standards Council, Glossary.)

E. **Computer Security Incident** - A violation, or imminent threat of violation, of computer security policies, acceptable use policies, and/or a disruption of network operations.

F. **Computer System(s)** – Computer system(s) includes, but is not limited to, all of 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/or tablets.

G. **Data Custodian** - A person or team designated by the data owner to be responsible for managing the data in order to maintain its confidentiality, integrity, and availability.

H. **Data Owner** – A 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.

I. **Disaster Recovery (DR)** – DR is the process, policies, and procedures related to preparing for recovery and/or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

J. **Dual Factor Authentication** – A security process in which the user provides two different authentication factors, for example, a password and a one-time passcode, to verify the user's identity.

K. **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 the computer systems, and vice versa, must pass through the firewall.

2. Only authorized traffic, as defined by the security policy, is allowed to pass through the firewall.

3. The system itself is immune to penetration by general standards.

L. **Mobile Device** – A handheld device or a mobile device is a small computing device that has an operating system and can run application software programs.

M. **Need to Know** - Known as "least privilege," need to know is the principle that requires each subject to 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.

N. **Payment Card Industry (PCI)** - Businesses or entities that process payments using debit cards, credit cards, and/or other payment cards.

O. **PCI Compliance** – Adherence to the PCI, Data Security Standards (DSS), a set of information security standards mandated by the PCI and administered by the Payment Card Industry Security Standard Council (PCISSC).

P. **Qualified Security Assessor (QSA)** - “Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the PCISSC to validate an entity’s adherence to PCI DSS. QSA employees are individuals who are employed by a QSA company and have satisfied and continue to satisfy all QSA requirements.” (PCISSC, “Qualified Security Assessor.”)

Q. **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.

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

S. **Users** - All individuals who have access to FCPS computing resources.

IV. Ownership and Responsibility

A. **School Board and the Leadership Team** - The School Board, Division 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 divisionwide information security program is implemented, effective, and well-supported with resources.

B. **Assistant Superintendent of Information Technology -** The assistant superintendent of Information Technology (IT) is responsible for the planning, budgeting, and performance of data security components. The assistant superintendent of IT 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.

C. **System and Data Sponsors and Owners –** Sponsors and/or owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of systems and information. Sponsors and/or owners 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 sponsors or owners for the respective systems and information in their custody.

D. **Systems and Data Custodians or Administrators -** System and data custodians and/or administrators 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 assigned. 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. PCI Security Standards

Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources, defines the acceptable use policy for all FCPS users.

A. **Account Management**

The system sponsor is the owner of the accounts on his and/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 and/or her account and preventing it from being misused. A user shall never allow others to use his and/or her account(s).

An account shall uniquely identify each user. Generic accounts are not allowed; any exceptions must be approved by IT senior management. Vendor-supplied default account credentials must be changed before deployment. The need to know principle shall be used to assign access rights to user accounts. The account provisioning process shall be recorded. Upon change or loss of need to know, user accounts and accesses shall be promptly modified or terminated.

An account shall be secured by at least one authentication factor that meets the FCPS standard (Section V.N.). Account logon and logoff shall be audited. The maximum logon attempts are six with a minimum of 30 minutes of lockout time and an idle timeout of 15 minutes shall be enforced.

An account that is used to log into a card data environment (CDE) shall be protected with dual factor authentication.

A cloud-based virtual machine (VM) uses FCPS domain accounts. Access shall be provisioned to the following Adult and Community Use (ACE) employee positions, based on the need to know principle: program administrator, financial analyst, finance technician, accounting technician, registration manager, program assistant, business operations assistant, business operations supervisor, administrative assistant, functional applications technician I/II/III, functional applications specialist I/II, and educational counselor.

Whenever there is a personnel change, program managers shall initiate processes to modify account access. Accounts shall be audited every 90 days by personnel designated by system sponsors.

For additional information, see Technical Bulletin 625, Lifecycle of FCPS Domain Accounts.

B. Application Standard

All credit card payment processing must be re-directed to a PCI-compliant payment gateway. FCPS 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%2020180607.htm. This link is available only through computers within the internal FCPS network, FCPSnet.

C. Audit

An annual audit shall be conducted by designated FCPS personnel or a third-party vendor on the PCI information security policy and network and data flow diagram.

PCI Security Standards are a compilation of numerous standards, each developed for its specific environment. Self-assessment questionnaire (SAQ-A) has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data. SAQ-C-VT (virtual terminal) has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet.

PCI SAQ-A and SAQ-C-VT shall be completed annually, and evidence shall be maintained. Periodically, a QSA shall be engaged to conduct the audit and sign-off on the SAQ-A and SAQ-C-VT.

D. Backup

Backups shall be performed for all PCI 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. For more information, please see Regulation 6221, Data Backups, Data Processing Recovery, and Contingency Planning; and Technical Bulletin 405, Electronic Backup Policy and Retention Schedule.

E. Critical System Change Management

Changes, both scheduled and unscheduled, to mission-critical systems and their computing environment facility shall follow the change management process. For more information, please see Regulation 6405, Change Management Process, and Technical Bulletin 301, Change Management Process.

F. DR and BCP

Information Technology Operations is responsible for developing, maintaining, and implementing a disaster recovery (DR) and business continuity plan (BCP) 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. For more information, please see Regulation 6405.

G. **File Integrity Monitoring**

File integrity monitoring is implemented for applicable components of the systems connected to the payment processing gateway.

H. **File Storage**

With the only exception of the last four (4) digits of the primary account number (PAN), payment card information such as PAN or card verification value (CVV) must *never* be stored by FCPS in any electronic format.

I. **Firewall**

IT Network and Systems Services (IT-NSS), is the system owner and custodian of all firewalls on the FCPS network as well as cloud services firewalls within FCPS. In addition, standards established in DIT Technical Bulletin 621, Fairfax County Public Schools Border Firewall Policy, a firewall that is used to protect the network segment that hosts the cardholder data environment must meet the following additional requirements:

1. Deny both inbound and outbound traffic by default.

2. Allow only approved traffic through the firewall.

3. Audit inbound and outbound traffic, as well as administrative access.

4. Document allowed traffic, specifying source, destination, and protocol.

J. **Host Security**

Payment card information shall only be handled on a designated cloud-based virtual machine. Neither personal devices nor end-user messaging technology such as email or short message service (SMS) messaging shall be used to transport PAN. The host shall be hardened in accordance with NIST800-123 standards:

1. Must have the current operating system (OS) patches and malware definition files.

2. All default passwords must be changed, including default simple network management protocol (SNMP) community strings.

3. Unused services, applications, or default accounts shall be either deleted or disabled.

4. Assign access and permission based on the need to know principle.

K. **Incident Handling**

The following parties should all be notified immediately if a security breach involving PCI data and PCI-related systems occurs:

1. Program manager and/or system sponsor; and,

2. IT Network Security, ComputerSecurity@fcps.edu, and IT Service Desk, 703-503-1600.

IT Network Security shall conduct an incident investigation to determine the cause, impact, and initiate data recovery as needed. The program manager and/or system sponsor shall analyze and determine the communication strategies and the legal requirements (i.e. notifications to impacted parties and payment brands) and coordinate with the FCPS Division Counsel office when applicable.

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

For more information, please refer to Technical Bulletin 611, Fairfax County Public School Security Incident Handling Procedures.

L. **Media Disposal**

When a computer is disposed, the data on the hard drives shall be destroyed before the computer leaves FCPS premises. Soft media, including but not limited to CDs, DVDs, floppy diskettes, JAZZ drives, ZIP drives, and memory sticks, shall be destroyed when the media is disposed of. For more information, please refer to Technical Bulletin 612, Fairfax County Public Schools (FCPS) Digital Media Disposal Procedures.

Paper records containing payment card information shall be retained for a minimum of one year and shall be destroyed at the end of their life cycle. Paper records must be transported in a secured container and they must be crosscut shredded.

For more information, please see Records Management Manual: https://www.fcps.edu/sites/default/files/media/forms/rmm.pdf

M. **Mobile Devices**

Neither FCPS-issued nor privately-owned mobile phones or tablets shall be used to process cardholder information for FCPS business except when authorized by IT.

N. **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. For more information, please see Technical Bulletin 633, Fairfax County Public Schools Network Device Security Standards.

O. **Passwords**

FCPS users are responsible for the security of their passwords and they must not reveal their passwords to others. FCPS technical support staff members will not ask a user for his and/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, or any other character strings with characteristics that may identify the user.

P. **Patch Management**

The operating systems as well as application software must have processes and procedures to install up-to-date security patches, when applicable.

Q. **Physical Security**

Paper records containing payment card information must be stored in a physically-secured area. Measures (locks, badges, keycards, etc.) shall be implemented to restrict access to an area. The program manager and/or administrator is responsible for granting and removing access to the controlled area, and provisioning of the access shall be documented. Access to the area shall be authorized to the following ACE employees on a need to know basis, and access promptly removed upon the loss of need to know: program administrator, financial analyst, finance technician, accounting technician, registration manager, program assistant, business operations assistant, business operations supervisor, and/or administrative assistant.

Visitors are not allowed to access the secure facility.

An inventory record of the paper records shall be maintained and periodically audited.

R. **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 comply with all FCPS policies and regulations.

A 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. For more information, please see Technical Bulletin 631, Fairfax County Public Schools Remote Access Policy.

S. **Security Awareness and Training Program**

All users that access FCPS network resources shall accept the FCPS acceptable use policy and receive security awareness training. FCPS users who handle PCI information shall receive additional PCI-specific security training annually. Training shall be documented and tracked**.**

T. **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. Please see Technical Bulletin 636, Fairfax County Public Schools Server Security Standards, for more information.

U. **Service Provider Management**

All vendors who provide payment card processing services shall be PCI compliant. System sponsors shall be responsible for designating appropriate FCPS personnel to check and ensure the compliance status annually. Agreements shall be established between FCPS and the vendors to state that the vendor will adhere to PCI standards while handling FCPS PCI information.

V. **Transport Security**

Use of strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over an open, public network are to include, but are not limited to the following: trust keys and certificates that are signed by certificate authorities and approved by the system sponsor; secure configuration of the protocol; and encryption strength that is appropriate for the methodology.

W. **Use of Privately-Owned Equipment**

Only designated FCPS-owned equipment may be used when entering or processing payment card information.

X. **Virus Protection**

All servers and workstations connected to the FCPS network or that perform FCPS business functions must perform system updates and use a virus protection program approved by IT. Users should not disable virus protection or system updates at any time.

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

Emails found with viruses and/or suspicious files shall be removed from the delivery system. Any device found with a virus must be taken off the network immediately until it has been cleaned and is verified as virus-free. Systems that cannot be cleaned will be reimaged. IT has the discretion to block network traffic that appears suspicious of carrying any form of virus.

Y. **Vulnerability Assessment**

Vulnerability assessment shall be conducted annually against the systems that process payment card information. Industry-standard assessment tools shall be used and risk rating shall be assigned based on reputable sources such as, common vulnerability scoring system (CVSS), score, and/or vendor (i.e. Microsoft) recommendation. At a minimum, findings with a risk rating of high and above shall be addressed.

Z. **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 or unauthorized access points are prohibited.

Configurations of the access points (APs) must adhere to the standards set forth by IT. IT will only maintain approved APs and reserves the right to disconnect any AP that interrupts normal network operations. Sensitive information, including but not limited to student records, must be transmitted over an encrypted and authenticated wireless network. For more information, please see Technical Bulletin 641, Fairfax County Public Schools Stationary Wireless Access Point LAN.

Also see the current version of:

Regulation 6221, Data Backups, Data Processing Recovery, and Contingency Planning
Regulation 6225, FCPS Information Security Policy
Regulation 6405, Change Management Process

Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources

The following are only available via the FCPS Intranet:
http://fcpsnet.fcps.edu/it/offices/ito/computing_srvcs/tech_bulletins.shtml

Technical Bulletin 301, Change Management Process

Technical Bulletin 405, Electronic Backup Policy and Retention Schedule

Technical Bulletin 611, Fairfax County Public Schools' Security Incident Handling Procedures

Technical Bulletin 612, Fairfax County Public Schools (FCPS) Digital Media Disposal Procedures

Technical Bulletin 621, Fairfax County Public Schools Border Firewall Policy

Technical Bulletin 625, Lifecycle of FCPS Domain Accounts

Technical Bulletin 631, Fairfax County Public Schools Remote Access Policy

Technical Bulletin 636, Fairfax County Public Schools Server Security Standards

Technical Bulletin 641, Fairfax County Public Schools Stationary Wireless Access Point LAN

Records Management Manual, https://www.fcps.edu/sites/default/files/media/forms/rmm.pdf

National Institute of Standards and Technology, NIST800-123, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf