Fairfax County
VIRGINIA

INFORMATION TECHNOLOGY SECURITY POLICY

Rev8 - 2020

DEPARTMENT OF INFORMATION TECHNOLOGY

INFORMATION SECURITY OFFICE

Fairfax County
VIRGINIA

Information Technology Security Policy

CEX Procedural Memorandum 70-05

ISO Policy Publication 70-05.01 v8

MICHAEL T. DENT
Chief Cyber Security and Privacy Officer

GREGORY SCOTT
Chief Technology Officer

BRYAN HILL
County Executive

Fairfax County, Virginia
PROCEDURAL MEMORANDUM NO. 70-05

To: Agency Directors	**Date:** Revised May 28, 2020
	Reference: PM 70-05, Information Technology Security Policy, *May 28, 2020 revised.*
Initiated by: Department of Information Technology	**Approved by County Executive:**
Subject: Fairfax County Information Technology Security Policy	

PURPOSE

Fairfax County Government is highly dependent on the use of information technology, communications systems, and other cyber based resources for the effective management of government programs that deliver services and perform internal administrative functions. As such, and with heightened risks and vulnerabilities abound that could compromise technology and data - a constant threat -, the County provides for the availability, continuity, integrity, and confidentiality and privacy of its information and communications systems, as well as the associated data and content, to ensure operability through information technology (IT) security governance and policies. Information systems in the county include all IT systems and critical infrastructure to include computers and communications equipment fixed or mobile, software, systems, applications, internet access, and the data and information contained or passing through them, and activities and individual behavior involving the use or management of the systems and information, i.e. actions and procedures that govern design, build, operate and maintain to create, collect, record, process, store, retrieve, display and transmit information (see Fairfax County ***Information Technology Security Policy*** for definitions). This also includes audio and video streaming and content; use of the Internet and any WEB based new media venues (*Social Media*), cloud services or other external information technology resources hosted by a third-party on behalf of the county, and similar capabilities; the County's WEB addresses (URLs) and image; wireless and remote access into the County's technology environment from anywhere; automated/industrial/mechanical/building management systems and other emerging network-enabled technologies commonly referred to as the "Internet Of Things"; cyber-ware, tools and interfaces that enable the county's information systems to be interoperable with external systems, and any technology capability in the future (all listed above herein referred to as 'IT Assets'). This procedural memorandum defines the policy for risk mitigating measures that govern the use of the County's IT Assets, and compliance requirements.

SCOPE

The Fairfax County Government Information Technology Security Policy ('the Policy') defines the minimum-security requirements for the protection of Fairfax County Government IT Assets, including the managerial, operational, and technical protection requirement and controls to ensure the confidentiality, integrity, and availability of County IT Assets; compliance with requirements of applicable federal, state, and local law and County policies and regulations (e.g. HIPAA, PCI-DSS, PII and other specific privacy regulations current or established later); and standards and guidelines established by the National Institute of Standards and Technology (NIST), US Department of Homeland Security Cyber security guidelines, US CERT, and any other in the future. The Policy applies to all existing and future implementations of technology.

The Policy defines the acceptable use and management of internal and remote systems, services and information, and technical controls and procedures that govern the design, acquisition, implementation, administration and use of County systems that assist in mitigating risks due to evolving cyber threats and vulnerabilities.

The Policy recognizes that IT/cyber security for the County is achieved through clearly defined information security program requirements, education and compliance in the appropriate use of technology, the collective support and involvement of County leadership, the collective operation of the Department of Information Technology (DIT) and County agencies' security and privacy programs, and on-going diligence in updating protective measures and enforcement. Functional or programmatic policies and procedures may be developed for specific technology implementations or areas of concern.

The Policy applies to all County agencies, employees, volunteers, service providers, vendors, contractors, and commercial entities (may be referred to as 'users' in county IT policy and procedure documents) that develop, implement, administer, or use Fairfax County information and communications systems, data and information.

POLICY

Fairfax County Government's Information Technology Security Policy shall enforce protective measures and actions for all County information and communications systems either internal or external, that transmit, receive, or store confidential, sensitive, internal use, or public use County data and/or information regardless of media format, processing method, mobility, or platform.

IT assets across all County IT platforms and infrastructure will be protected throughout the system lifecycle by implementing IT system management policies and procedures, and IT and cyber-security protective measures that meet applicable federal, state, local, other regulatory, and contractual requirements and support the County's mission, vision, ethics and values. In the event that standards and guidelines for a particular technology or procedure are not specifically defined in this or other governing County IT Policies, users shall follow the basic principles of information systems security and apply caution in all efforts to safeguard Fairfax County Government information and systems.

All agencies and persons that may develop, implement, or use Fairfax County information systems shall abide by the requirements and procedures established by the County's Information Technology Security Office as authorized by the County Executive. Any information, data, or any other content that is in or transmitted through Fairfax County IT platforms, communications systems and infrastructure including through County external sources such as Internet based, County Social Media venues, subscription and 'Cloud' services is the property of Fairfax County, thus users should not expect that personal information conducted through the county is private other than data explicitly covered by confidentiality and privacy laws. County data deemed sensitive may not be published on personal Social Media venues or personal storage media or such as provisioned through personal wireless accounts unless permission is specifically granted. Individuals may not use access from the county IT environment or devices to conduct any illegal or offensive acts to any personal venues, such as in Social Media. This policy supersedes any previous policies that may be in conflict and acts a minimum standard for agencies' specific policies.

GOVERNANCE

Fairfax County Government's Senior Information Technology Steering Committee (Sr. IT), composed of the County Executive, Deputy County Executives, Chief Financial Officer (CFO), and the Chief Technology Officer (CTO) is responsible for overall governance of the County's Information Technology program, and determines acceptable level of risk and related exposures to the County in the development of IT/cyber-security policy, practices and investments. The CTO implements the committee's decisions and shall authorize necessary protective measures for IT enterprise wide.

As authorized by the County Executive, and under the CTO's guidance, the Chief Information Security Officer (CISO) and the DIT Information Security Office (ISO) shall be responsible for guiding, implementing, assessing, and maintaining Fairfax County Government's information security posture and this Policy in accordance with the defined information security program. The CISO is authorized to conduct routine monitoring of systems, use, and enforce compliance directly.

COMPLIANCE

This policy shall serve as an adequacy standard for information security safeguards and shall form the basis on which information security audits and reviews will be conducted. All activity from the county's IT environments and on county computer resources is subject to monitoring by authorized staff or designates to ensure system integrity and compliance with information security policy, related standards, and governing statutes. The ISO also may disable use privileges and systems found introducing unacceptable risk and the related exposures to the County. Disciplinary matters resulting from violation of information security policies are coordinated with the source offending agency and the Department of Human Resources. Due to the seriousness of harm to the Fairfax County's assets, integrity of its operations and information, and cost of damage caused by IT security breaches, misuse and intentional violation of IT security policy and controls will not be tolerated, and may be subject to applicable disciplinary measures and, or further subject to criminal prosecution or civil adjudication.

RESPONSIBILITY

The responsibility for implementation of the security policy compliance resides with all employees and other users and at all levels of the County organization. Detailed responsibilities are outlined in the DIT Information Technology Security Policy and program documentation.

EXCEPTIONS TO POLICY

Exceptions to Fairfax County Government's information security policies may be requested. A DIT Information Security Office Request for Policy Exception/Waiver Form shall be prepared by the agency, signed by the agency head or designee, and submitted for review and determination by the CISO and CTO. Certain exception requests may require escalation to the County Executive whose responsibilities include DIT, e-Government, and HIPAA functions for determination. Periodic reviews of all granted exceptions will be conducted by the CISO and reviewed by the CTO or Deputy County Executive to ensure that the original business need is still valid, and the risk level is still acceptable. Note: There are no exceptions to the Vulnerability Management section of the policy.

REVISIONS

Fairfax County Information Technology Security Policy is guided by the classification of County information based on law and regulation, information sensitivity levels, and internal protocols. This policy maps to existing policy categories in NIST special publication 800-53: *Recommended Security Controls for Federal Information Systems and Organizations and* may periodically be revised as necessitated by future federal and state legislation and/or publications or as necessitated.

REFERENCES:

CEX PM 70-05 (revised 2017)
Fairfax County Communications Policy
DIT Information Technology Security Policy
DIT ISO Office IT Security Program
NIST special publication 800-53
HIPAA, PCI-DSS, PII and Commonwealth of Virginia Privacy regulations
DIT Forms: *'IT Agreement for Employees', IT Agreement for Consultants, IT Security Request Forms; ISO Waiver forms, et al.*

TABLE OF CONTENTS

INTRODUCTION

Fairfax County Government progressively uses information technology for the effective management of government programs that deliver services to our constituency and regional partners, as well as to perform internal administrative functions. The County shall ensure the confidentiality, privacy, integrity, and availability of its information and communications systems and data through the governance of County information systems, critical communications and platform infrastructure and devices by implementing information security policies that meet federal, state, and local regulations and mitigate risk and vulnerabilities but also assist in meeting the business technology needs and requirements of our stakeholders.

The **Fairfax County Information Technology Security Policy ('Policy')** provides a foundation for the security program managerial, operational, and technical protection requirements and controls for agencies, entities that use information systems and communications capabilities in the Fairfax County domain, and end-users to ensure the confidentiality, privacy, integrity, and availability of County technology assets: information and data, systems, devices, and critical communications infrastructure as required by applicable federal, state, and local laws, and County policies, guidelines and regulations. It is designed to provide agencies and personnel the minimal requirements and guidance for securing County information and systems. Governance, roles and responsibilities, information classification, security monitoring, operational procedures, technical solutions, and enforcement are covered.

Information Technology is a tool by which County business is conducted, and behavior in its use is likewise implicit in County Human Resources policies, Employee Handbook, Standards of Conduct, Code of Ethics, Communications Policy, Social Media Policy and any other County governing policies that may be implemented in the future that define use of technical capabilities, information and data. This Policy provides the baseline for implementation of information security enterprise-wide that includes Department of Information Technology (DIT) IT policies and procedures, other related County-wide policies, and County agency-specific system management and IT security policies and procedures.

The Policy defines the security program managerial, operational, and technical protection requirements and controls for agencies to ensure the confidentiality, privacy, integrity, and availability of County information and data, systems, devices and critical communications infrastructure as required by applicable federal, state, and local laws, County policies and regulations, and contractual obligations. This applies to all IT assets – capital or leased, and communications capabilities – county private or commercially provided, non-traditional "Internet of Things" (IoT) products intended to integrate with County enterprise infrastructure, contracts and contracted managed services (hosted, "cloud", and/or shared services/SaaS solutions, etc.). In addition, the policy defines acceptable use of County information technology resources by County employees, State Employees, contractors, volunteers, vendors, and temporary staff.

The Policy recognizes that information security for the County can only be achieved through clearly defined business objectives, technology standards, information security program requirements, awareness and education of users for appropriate use of technology, the collective support and involvement of County leadership, and enforcement.

The Policy also defines the acceptable use and management of internal and remote systems, and Internet based resources and capabilities (including 'social media'; any similar next generation IT capability), wireless and mobile apps, content sources, and procedures that govern the design, implementation, use and administration of County systems, data and information in order to mitigating risk of evolving threats and vulnerabilities to technology, either technologically or through actions (human behavior bourn).

SCOPE

Fairfax County Information Technology Security Policy shall provide the minimum requirement and enforce protective measures for **all information and systems** that transmit, receive, or store Confidential, Sensitive, Internal use, or Public Use information regardless of electronic or digital media format, processing method, or platform, for or interactive with Fairfax County unless otherwise determined. If specific standards and guidelines for a technology or procedure are not specifically mentioned in this **Policy**, user shall assume that any capability whereby information and data flows automated now and in the future internally or externally shall follow the defined principles of information systems security and apply caution in all efforts to safeguard Fairfax County Government information and systems.

The county uses the National Institute of Standards and Technology (NIST), which is for Federal Systems and Organizations, as a guide and best practices example. The County strives to implement NSIT Standards to the extent practicable for local government enterprises.

The Information Technology Security Policy shall apply to:

- **All County agencies to include authorities, legislative and judicial administrative agencies, and any department or organization attached to the Fairfax County technology enterprise or receiving county resources supporting their technology assets and programs, herein referred to as 'agencies', employees, volunteers, service providers, vendors, contractors, and commercial entities** that develop, implement, administer, or use Fairfax County information systems.

- **All existing and future implementations of information systems, communications, other technology and the Internet** at Fairfax County Government or in use interoperability capabilities with partner organizations. This includes **personally owned devices** authorized for use with Fairfax County systems and covered data. Information assets across all platforms used by the Fairfax County Government will be protected throughout the system lifecycle.

GOVERNANCE

The Policy is implemented and enforced by the Chief Cyber Security and Privacy Officer of Fairfax County, and the Department of Information Technology by authority of the County Executive. **County Procedural Memorandum No. 70-05** is the authorizing document for this policy. All agency heads are expected to incorporate practices in their operations in alignment with this policy.

Fairfax County Information Technology Steering Committee, composed of the County Executive, Deputy County Executives, Chief Financial Officer, and the Chief Technology Officer shall be responsible for overall governance of the County's Information Security Program, determine acceptable risk levels to County information and systems, and authorize necessary protection requirements. Enforcement of policy is the direct authority of the County Executive.

Under the County Executive's authority and the Chief Technology Officer's guidance, the Chief Cyber Security and Privacy Officer and the DIT Information Security Office shall be responsible for guiding, implementing, assessing, and maintaining Fairfax County Government's information security posture in accordance with the defined Information Security program.

EXCEPTIONS TO POLICY

Exceptions to information security policies may be requested. A ***DIT Information Security Office Request for Policy Exception/Waiver Form*** shall be prepared by the agency, signed by the agency head or their designee, and submitted for review and determination by the CCSPO and CTO. Certain exception requests may require escalation to the County Executive for determination. Periodic reviews of all granted exceptions will be conducted by the CCSPO to ensure that the original business need is still valid, and the risk level is still acceptable.

KEY TERMS

Privacy: control over the extent, timing, and circumstances of sharing oneself – physically, behaviorally, or intellectually with others. Typically is related to individual autonomy and a person's constitutional right to control their own information, including decisions of when and whether to share personal information, how much information to share, the circumstances under which that information can be shared, and with whom it should be shared.

Confidentiality: the nondisclosure of information except to authorized individuals. Typically relates to the legal obligations of a public or private sector entity to safeguard information in which it has been entrusted.

Integrity: condition of undiminished accuracy, reliability, and protection from unauthorized access or modification.

Availability: reliable and timely access to data, systems, and resources.

Personally Identifiable Information (PII): information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Examples include name, social security number, date or place of birth, mother's maiden name, and other information.

Information Security: practice of safeguarding an organization's information from unauthorized access, modification, or destruction.

Cyber Security: A branch of information security that encompasses procedures, practices, and measures taken to protect networks and systems connected to the internet from compromises affecting confidentiality, integrity, and availability.

Information Security Policy: policy that explains how an organization plans to protect information technology (IT) assets. Information security policies typically contain rules that discuss information and system protection requirements and standards, security and network operational guidelines, incident response procedures, the acceptable use of systems, and the enforcement of compliance with regulations and legislation.

Vulnerability: software, hardware or procedural weakness that may compromise the confidentiality, integrity, and availability of information and systems.

Threat: any potential danger to information and systems. Examples of some threats may include malicious code, viruses, network attacks, operational weaknesses and vulnerabilities, intentional or inadvertent personnel actions, and natural events.

Risk: the capability and likelihood of a threat or vulnerability compromising the confidentiality, integrity and availability of information and systems. Risk analysis evaluates the probability of a vulnerability or threat resulting in an unfavorable business impact.

Countermeasure: safeguard put into place to mitigate risk to information and systems. Examples of technical countermeasures may include firewalls, intrusion prevention systems and access control mechanisms. Operational countermeasures may include change and configuration management, security awareness training, and written policies.

ROLES AND RESPONSIBILITIES

Implementing the policies defined in the County Information Security Program shall be a cohesive effort involving all levels of Fairfax County Government leadership, management and personnel. Roles of agencies and personnel involved in the implementation of information technology and Fairfax County's IT Security Program are described below.

Department of Information Technology (DIT)

DIT is the authorized agency for planning, design and implementation of information technology and communications systems for the County enterprise to include, but not limited to, designing, deploying and administering information systems, applications, network infrastructure, telephony, mobile communications and devices, websites and data storage, and any other information technology now or in the future. DIT shall implement information systems, applications, and other devices according to existing policies, standards, and procedures, and assist in the development of information systems policies, standards, architectures, procedures, organizational structures, and other management tools to be consistent with industry best practices and legal requirements. DIT is the primary custodian of data and information for agencies; however, agencies are the owners of their data and are required to provide appropriate stewardship and lifecycle management.

Information Security Office (DIT ISO)

The Chief Cyber Security and Privacy Officer leads the County-wide Information Security Office, which is in DIT, and shall implement the requirements of the Fairfax County Information Technology Information Security Program. ISO shall develop security policy in accordance with County policies and standards and laws, provide information security consultation and guidance to County agencies and departments, conduct incident response, manage enterprise security devices and applications, and act on incidents and violations.

The DIT Information Security Office shall or compel agencies to perform audits, and security and risk assessments to determine the adequacy and effectiveness of security controls and ensure systems are designed, configured, tested, operated, and administered in a manner which is consistent with legal regulations and County standards and policies. Audits, traces and scans may be on-going and without prior notice.

The county may have a Privacy Officer that works on Heath Information Privacy and Portability Act (HIPAA), Personally Identifiable Information (PII), Procurement Card Industry (PCI) and/or any other compliance requirements for identified sensitive information. This position works with agencies and with ISO for its activities. Data owner are responsible for the meeting the requirements for data privacy irrespective of having a formal privacy officer.

Architecture Review Board (ARB)

The ARB is a group of DIT managers/senior experts across IT specialties tasked with the oversight, regulation, and compliance of County information systems to architectural, platform, and data standards and principles to ensure data confidentiality, integrity, availability and compatibility from an enterprise architecture and standards compliance perspective. The ARB or designees are responsible for the establishment and publication of standards for information technology for use by County agencies when planning and developing IT projects and initiatives. The ARB is consultative, and reviews new solution requests/plans as needed for completeness and for compliance to enterprise-standards. ARB may grant Waiver recommendation for necessary third-party solutions as practicable.

Chief Technology Officer (CTO)

The CTO is the Director of the Department of Information Technology for Fairfax County. The CTO directs and manages County-wide investments in technology, IT operations, and ensures that processes are in place so that technical safeguards are available to secure electronic information in the implementation of technological solutions. The CTO maintains the authority to develop and implement enterprise-wide IT and IT security policies, standards, and procedures for all technology that may be implemented by DIT or agencies. Also, that the acquisition and implementation of IT systems includes approved IT security methods, both technically and functionally, and is coordinated and integrated as part of the development of technology initiatives. The CTO establishes the IT Security Office, and the position of Chief Cyber Security and Privacy Officer. The development, integration, and enforcement of the information technology security policy are the responsibility of the Chief Cyber Security and Privacy Officer, reporting to the CTO.

Chief Cyber Security and Privacy Officer (CCSPO)

Under the authority of the County Executive, and administrative supervision of the Information Officer (CTO), the Chief Cyber Security and Privacy Officer is the most senior cyber security, privacy and IT risk official for the County with responsibility over the protection of the county-wide technology assets to include networks, systems, applications, data and information, industrial control systems, automated systems and devices, the Internet and commercially provided information services. Serves as advisor to Board of Supervisors, County Executive, Agency Heads and Fairfax County Public Schools for all strategic business endeavors associated with IoT, ‘Smart Communities’, and any technology driven initiatives. Develops and implements the vision, strategy, and programs necessary to ensure information assets, technologies and data and supporting architecture are adequately secured. The CCSPO is a member of the DIT senior leadership team and is in line of succession after Deputy Directors for the CTO/Director of DIT. Serves as the principle advisor to the County Executive and Chief Technology Officer (CTO) on information protection and cyber matters, and represents Fairfax County on regional, state and federal committees and councils, and at industry venues.

IT Security Program Director

In the Department of Information Technology and under the general supervision of the Chief Cyber Security and Privacy Officer, the IT Security Program Director has responsibility to direct daily countywide information security and privacy efforts through the Information Security office (ISO), Department of Information Technology, and Agency Information Security Coordinators (AISC). The IT Security Program Director manages daily cyber security operations within the Information Security Office and is responsible for implementing cyber security policies, standards, practices, and technology solutions designed to protect the county technology environment, infrastructure, and data.

Office of the Internal Auditor

The Office of the Internal Auditor (IA) may conduct periodic reviews of County-wide as well as agency specific systems and practices assurance related to IT Security and Information Protection policies and procedures and may make recommendations related to best practices. The system audit goal is for ensuring that agency information and systems are adequately secured through risk management strategies and in compliance with all applicable laws, regulations, policies, standards, and procedural controls. The systems audit security assessments are designed to identify risk and gaps and ensure compliance. The audit will consider whether employees have been assigned specific responsibility and accountability for information systems related controls as part of their duties in managing information systems and may make specific recommendations for clarifying and assigning both responsibility and accountability.

ENFORCEMENT AND VIOLATION HANDLING

The **Chief Cyber Security and Privacy Officer** and the **Office of the Internal Auditor (IA)** will periodically review the progress of agency information security programs and practices and with the Department of Information Technology and/or conduct investigations to ensure compliance of all County information systems and resources. Further, the independent external auditor will review security processes and controls for the enterprise-wide financial, human resources and procurement system – FOCUS, and other systems that process county monies such as tax and revenue systems in their annual audit work. Outcomes from audit work of ISO, IA or independent auditors can be in the form of:

- Findings with recommendations whereby there exists opportunities for strengthening procedures and controls;
- Findings with a requirement for implementing controls;
- Recommendation for remediation of discovered vulnerabilities;
- Personnel or contractual actions based on violations, breach of policy or enterprise, or for cause of significant threats.

Enforcement of this policy, including development of more specific procedures and guidelines which are agency-specific, shall be the local responsibility of each agency. Violations of this security policy shall be reported to the appropriate agency management and the CCSPO. Fairfax County Government shall conduct regular audits and actively monitor for violations of this policy.

Violations may be defined as an act or event that exposes the County or agency to actual or potential damage through the compromise of information systems security, the disclosure of sensitive or confidential information, the unauthorized use of agency data or resources, and the use of information systems for personal gain, unethical, harmful, or illicit purposes. Other events defined as violations may include, but are not limited to, the theft, loss, unauthorized use or misuse, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denial of service of County information or information systems.

The Fairfax County **Procedural Memorandum #02-04: Fraud Policy** shall be used as a guideline for determining a course of action if a violation indicates potential fraud.

Fairfax County Government personnel regulations require that employees abide by applicable laws, regulations, and standards of conduct. Intentional violations, regardless of the number of violations, may result in disciplinary action up to and including termination. Fairfax County Government maintains the right to refer information security incidents to external authorities and to seek legal action against personnel that misuse County information systems in a manner that violates law and applicable policy.

Fairfax County Government shall maintain the right to sever contracts and agreements with contractors and external entities that violate this policy or demonstrate conduct that impacts the confidentiality, integrity, and availability of County information and systems.

The Fairfax County CTO and CCSPO are authorized to institute any necessary measures to enforce and manage the compliance of County information systems. This may include disconnecting systems that introduce unacceptable risks and vulnerabilities to County information, disabling user privileges, and revoking or disabling user accounts.

COUNTY AGENCIES' & OTHER USER ENTITIES INVOLVEMENT AND RESPONSIBILITIES

The continuous commitment and involvement of County agency leadership is a prerequisite for an effective information technology security program. The Fairfax County IT Security Policy requires agency leadership to maintain vigilance in executing and ensuring compliance with the appropriate controls as prescribed in this policy. Agency heads are expected to be ambassadors of County policy and demonstrate diligence in compliance in their use and their agencies compliance of this policy.

Agency Head

The Agency Head is ultimately responsible for incorporating and implementing the Information Technology Security Policy and program in their agencies and ensuring that all agency information system, regardless of medium, are used, maintained, disclosed and disposed of according to law, regulation, policy, and standards. The Agency Head maintains the authority and accountability to implement subordinate agency information security policies, standards, and procedures to enhance protection of agency information systems, but shall not detract from the County's security policy and program. Agency Heads shall ensure user awareness of security policy, acceptable use, standards, guidelines, and procedures.

The Agency Head shall appoint an Agency Information Security Coordinator (AISC) to implement and maintain the information security program within their agency. The appointed person's position description shall include this responsibility and the function will be assessed during performance evaluations. Based on the responsibilities and requirements of the AISC function, it is expected that the AISC role will be performed by staff in a professional series such as a Business Analyst, Management Analyst, or Network/Telecommunications Analyst, rather than administrative level personnel. Additionally, the Agency Head shall designate an Agency Access Control Administrator (AACA) for access control administrative activities required by the Information Technology Security Policy and these activities may be performed by administrative level staff. The Agency Head shall appoint both a Financial/Procurement Application Approver and a Human Resources Application Approver (FPAA/HRAA) for access control related to FOCUS account administration, these activities should be performed by staff within an agency responsible for budget/fiscal management, procurement processing, or human resources management. Any agency program manager or other responsible position is required to notify the ISO and the Agency Head of any necessary immediate action needed as a result of a Policy violation or security incident so that access can be disabled or reviewed. This may be also through the AISC or AACA.

Agency management's responsibilities shall include the following:

- Designating Agency Information Security Contacts:
    - **Agency Information Security Coordinator (AISC**) who shall administer the information technology security function at the agency. *(It is highly recommended that personnel appointed to perform **AISC** duties be selected from a professional level employment series with knowledge of information technology, information security, and knowledge of department or agency specific business requirements and operations).*

  - **Agency Access Control Administrator (AACA)** who shall administer user access control privileges as authorized. (***AACA** are typically administrative support personnel or (formerly agency mainframe administrator), who administer the hiring and access control process in agencies, or another designee).*
  - **Financial/Procurement Access Approver (FPAA)** who shall request, approve and audit Financial and Procurement related access for the FOCUS system. *(The FPAA must be budget/fiscal or procurement management staff and be familiar with the Financial and Procurement operational roles within the agency.)*
  - **Human Resource Access Approver (HRAA)** who shall request, approve and audit Human Resources related access for the FOCUS system. *(The HRAA must be a designated HR Manager per the Department of Human Resources and be familiar with the Human Resource operational roles within the agency)*

- Ensuring that the security function within the agency hierarchy has the shortest practicable reporting lines to the agency head, or similarly leveled designee.

- Ensuring Agency IT Analysts sign 'IT Employee Agreement', and that their consultants that preform IT work sign the 'IT Consultant Agreement' (*sample in appendix*).

- Developing an agency-specific IT Security Policy anchored to the agency's business needs and in compliance with the County's IT Security Policy and enterprise-wide IT and other policies.

- Ensuring clear lines of communication between agency information technology managers and/or analysts and organizational general users about security matters and enforcement, and the Fairfax County IT Security Office and Department of Information Technology

- Implementing and maintaining procedures that ensure information system resources and data are protected in accordance with Fairfax County policy and standards, and applicable Commonwealth and federal laws, policies, mandates, standards and guidelines.

- Establishing an agency information security awareness program and ensuring that IT Security Training is promoted as part of agencies' employees' training requirements.

- Embedding IT security fundamentals within business practices that use information systems.

- Determining acceptable risk and establishing a process for business impact analyses, risk assessments, controls adequacy and develop a business continuity plan.

- Review required reports related to access and system activity for the agencies users.

- Conducting enforcement by notifying the IT Security Office and/or Department of Human Resources of policy violations and security incidents.

Agency Information Security Coordinator (AISC)

The AISC is responsible for administering the information security functions within the agency as appointed by the agency head and is the initial point of contact at the agency for all information security matters. The AISC is responsible for implementing and maintaining the Information Security Program to include coordinating the development and maintenance of agency-specific information security policies, standards, and procedures. The AISC is responsible for providing information security advice and recommendations to users and management within their agency. The AISC is responsible for receiving and disseminating network alerts, outage notifications, or other issues affecting the agency. The AISC should be familiar with local business conditions including prevailing laws, organizational culture, and the information systems that support operations. The AISC may also be required to install, operate, monitor, maintain, and manage certain security controls within their department such as data classification and access, establishment of agency-specific procedures for access control administration, security log reviews, and password resets. The AISC may delegate access control and administrative tasks to personnel formally designated as the Agency Access Control Administrator. It is highly recommended that personnel appointed to perform AISC duties be selected from a professional level employment series with knowledge of information technology, information security, and knowledge of department or agency specific business requirements and operations.

Agency Access Control Administrator (AACA)

The AACA typically coordinates the provisioning of user access to enterprise-wide network systems with DIT and may also coordinate for their agency for access to agency-owned information systems. The enterprise access that DIT enables includes mainframe and Active Directory and network access, and FairfaxNET and Exchange/Outlook (or future enterprise messaging systems).

The AACA is responsible for maintaining accurate and current access control records reflecting user contact information, privileges, and management authorization. The administrator is responsible for immediately terminating user privileges when workers change jobs or leave the County and notifying DIT of such action. This would typically be automated through IDM and FOCUS with the normal personnel action system updates; however, for immediate actions necessitated by an incident, the ISO will be notified by the AACA or agency authority immediately.

The AACA is responsible for ensuring agency users have only the access needed to perform their assigned duties. Under general oversight of the AISC, the AACA may be required to install, operate, monitor, maintain, and manage certain security controls within their department such as data classification and access, establishment of agency-specific procedures for access control administration, security log reviews, and password resets.

Financial/Procurement and Human Resources Application Approver (FPAA, HRAA)

Financial/Procurement and Human Resources Application Approvers coordinate, submit and approve access related to the County's Enterprise Financial/Procurement and Human Resource system, FOCUS.

The FPAA and HRAA are responsible for maintaining accurate and current access control records reflecting user contact information, privileges, and management authorization. The administrator is responsible for validating immediate termination of user privileges when workers change jobs or leave the County. This would typically be automated through IDM and FOCUS with the normal personnel action system updates; however, for immediate actions necessitated by an incident, the ISO will be notified by the FPAA/HRAA or agency authority immediately.

The FPAA and HRAA are responsible for ensuring agency users have only the access needed to perform their assigned duties. Under general oversight of the AISC, the FPAA and HRAA may be required to establish an agency-specific procedure for access control administration, provide input to audits related to Financial/Procurement audits (FPAA) or Human Resource related audits (HRAA), security log reviews, and password resets if applicable.

Agency Application Owner

The Agency Application Owner is an administrator or application operator who takes responsibility for an application that is not managed by DIT. These applications may be single agency or for multiple agency use. The Agency Application Owner is responsible for the verification that the application meets all DIT requirements and standards. They are also responsible for auditing of the systems access, ensuring the data is safe-guarded according to any applicable standards, including but not limited to HIPAA, PCI-DSS, and PII.

Program Manager

The Program Manager is the business professional responsible for the County information and whose focus is the achievement of business objectives regardless of the technology used to achieve the objectives. The Program Manager is assigned ownership of County business process and information systems in their agency and is responsible for maintaining the integrity of the information used in their systems, programs and projects.

Technical Manager

The Technical Manager is the assigned administrative custodian of information systems and is responsible for planning, design and execution of activities for the implementation and administration of those systems. The Technical Manager assists agency program managers in the determination of effective controls to be used to protect the systems, information and data. The Technical Manager is responsible for implementing techniques and procedures for detecting, investigating, and reporting breaches in information security.

Data and System Owner

Fairfax County Government information and systems are the property of Fairfax County. While this policy indicates that specific owners shall be identified, this ownership shall be custodial in nature. All production system information shall have a designated Owner. The Owner is the agency designee of the business functional area accountable for managing information assets and is responsible for implementing security controls such as user access and privileges. The Owner of a collection of information is responsible for the results and use of that business system or information. In situations where ownership is not explicit, the agency head shall assume ownership responsibility unless a specific Owner is designated.

Data and System Custodian

The Data and System Custodian is the guardian or caretaker of County data and is assigned by the agency or department to implement the protection requirements at the level classified by the Data Owner. Custodians are in physical or logical possession of either Fairfax County information or information systems that have been entrusted to the County. The custodian is responsible for maintaining the security measures defined by owners and they have operational-level responsibility for adequately protecting County information. Custodians include DIT personnel, local agency system administrators, and system users. All production application system information shall have one or more designated Custodians.

Custodians shall ensure the system properly audits events such as logins, file access, and security incidents. Custodians shall ensure processes are in place for the detection of security violations and monitor compliance with information security requirements.

Custodians define and implement processes for assigning user access codes, revoking user access privileges, configuring file protection parameters and implementing other data protection and access controls established by policy. Custodians shall also define and implement procedures for the backup and recovery of agency information. Custodians shall maintain records of those granted physical access to information assets and limit physical access to information assets, including maintaining documentation of equipment entering and leaving facilities, implementing authorization procedures prior to physical access, maintaining and archiving maintenance records, and sign-in documentation for visitors to be escorted.

System User

Authorized System Users are individuals who have been granted access to County information systems to perform assigned duties. Users may include, but are not limited to, merit and non-merit employees, vendors, contractors, volunteers, or other affiliates of Fairfax County Government. All users are responsible for protecting County information from unauthorized disclosure, modification, deletion and usage. Users shall comply with all applicable laws, regulations, policies, standards, and procedural controls in order to protect County information systems and shall report sensitive security issues, misuse, and violations of security policy to the AISC or CCSPO. Users shall be encouraged to make suggestions to improve the Information Technology Security Program.

GUIDING PRINCIPLES

The development of Information Technology Security Policy for Fairfax County Government shall be based upon the fundamental principles of information and system ownership and the legal obligations and requirements for protecting information and systems. Evolving threats and risks to information and systems due to changing technologies and access methods require policy to be flexible and adaptive, yet concise and consistent in defining user expectations, acceptable use, and boundaries.

Ownership

County information and systems are the property of the Fairfax County Government and are intended for official government use only. Fairfax County shall retain property rights to all information created, generated, replicated, processed, stored, transmitted, and received by users in the course of using County systems and software.

DIT shall be responsible for the acquisition, design, development, implementation, and administration of centrally managed information systems and resources and developing managerial, operational, and technical policy, processes, and procedures for governing and guiding information technology activities throughout County agencies.

Legal and Regulatory Requirements

Fairfax County information systems transmit, receive, process, and store information that shall be protected according to federal, state, and local laws and regulations. The development of an overarching security policy for Fairfax County, and the development of specific policy for County agencies shall take into consideration those laws and regulatory issues applicable to the operating environments.

Agencies that process information governed by the **Payment Card Industry** Data Security Standard (PCI-DSS) shall implement security standards to minimize risk of the unauthorized exposure of cardholder information and credit card fraud.

Fairfax County agencies that process, receive, maintain, or transmit electronic protected health information shall ensure the information is protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures by implementing the **Health Insurance Portability and Accountability Act** (HIPAA) Security Rule standards for information systems.

Agencies shall implement measures to protect any **Personally Identifiable Information** (PII) processed, transmitted, received, and stored on County information systems. The overall privacy of information are concerns both for individuals whose personal information is at stake and for agencies that may be liable or have their reputations damaged should PII be inappropriately accessed, used, or disclosed.

Additional laws and regulation which also govern the development of Fairfax County Information Technology Security Policy shall include the US Privacy Act, the Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, the Virginia Freedom of Information Act, the Virginia Government Data Collection and Dissemination Practices Act, and Virginia Security Breach Notification requirements.

The **Office of the County Attorney** shall make the determination of the application of Law and legal interpretation of issues as required in assisting the **Information Security Officer** in carrying out the duties and compliance responsibilities of this Policy. The **Privacy Compliance Manager** shall monitor and investigate matters involving HIPAA and PCI as well as other information privacy matters.

Information Classification

County agency leadership and data owners shall be responsible for determining data classification levels for information processed on County information systems based upon legal and regulatory requirements. Compliance with federal, state, and local laws dictate the managerial, operational, and technical controls to be implemented as part of this security policy.

Assigned classification levels to County information shall guide the development of applicable security policy, controls, and standards to ensure the confidentiality, integrity, and availability of the information.

Fairfax County Information shall be separated into the four pre-defined classes of Confidential, Sensitive, Internal Use, and Public Use in order to categorize data and convey the required safeguards for information.

Confidential

This classification applies to the most sensitive business information that is intended strictly for use within the organization. Confidential information is exempt from disclosure under the provisions of the Virginia Freedom of Information Act and other applicable federal and state laws and regulations. The unauthorized disclosure of Confidential information can substantially harm the interests of Fairfax County Government or cause severe financial, legal, or regulatory damage to Fairfax County Government, its customers, vendors, or employees. Compromise of confidential information could also prejudice the maintenance of law and order, impede the effective conduct of government, or violate the privacy of its citizens. For example, County critical infrastructure information, emergency response plans or weaknesses, information on County security weaknesses, passwords, or Private Health Information protected by HIPAA are considered Confidential.

Sensitive

This classification applies to information that requires special precautions in assuring the integrity of the information through protection from unauthorized modification or deletion.

Sensitive Information requires a higher than normal assurance of accuracy and completeness and needs to be protected because of public interest. Compromise of Sensitive information would likely damage the interests of Fairfax County Government or endanger the safety of its citizens. For example, Sensitive information might include information concerning County economic interests or project details.

Internal Use

This classification applies to information that is intended only for use within the organization. External access to this data should be prevented but compromises are not critical. Internal access is selective. Data integrity is important but not vital. Examples of Internal Use information may include employee training materials, contractor bid information (prior to contract being awarded), and internal policies, standards, or procedures.

Public Use

This classification applies to non-sensitive information. Public Use information does not require authentication, is available to the general public, and is intended for distribution outside the organization. Public Use information has been declared public knowledge by someone with the proper authorization and can disseminated without any possible damage to Fairfax County Government. Unauthorized disclosure is still against policy; however, it is not expected to seriously or adversely impact the organization, employees, or customers. Examples of Public Use information may include marketing brochures, advertisements, job announcements, and press releases that are available in the public domain.

Privacy

Fairfax County Government information systems users shall maintain no expectation of privacy while using County information systems. Fairfax County authorized personnel may monitor information systems, network infrastructure, and network traffic as deemed necessary to protect County information and systems.

Electronic records are official records of the Fairfax County Government and may be subject to release under the **Virginia Freedom of Information Act** and the **Virginia Government Data Collection and Dissemination Practices Act ("Privacy Act").**

Fairfax County Government shall reserve the right to audit networks, systems, and content to ensure compliance with this policy and conduct incident response. Fairfax County Government further reserves the right to perform forensic analysis of data and systems for authorized investigations into policy violations.

Electronic files created, transmitted, received, and stored on County information systems may be accessed by DIT authorized employees at any time based on a "need to know" or "need to access" without the consent of the information systems user.

Fairfax County information systems shall display a warning banner which identifies the system as a Fairfax County resource, indicates that system access is limited to authorized individuals, informs users that system and user activities are subject to monitoring, and that system or user access indicates an acknowledgment of these provisions.

Conduct and Acceptable Use

Fairfax County Government personnel regulations require that employees abide by applicable laws, regulations, and standards of conduct when using County information systems. Intentional violations of this policy, regardless of the number of violations, may result in disciplinary action up to and including termination. Fairfax County Government maintains the right to seek legal action against anyone who misuses County information systems in a manner that violates law and these policies. **Acceptable Use of County Information Systems** is included in Section 4.0 of this Policy**.**

The Policy is divided up into the following major sections:

Policy Section	Audience	Description
1.0 Management Policies	***Management***	*Describes County leadership responsibilities for guiding the Information Security Program*
2.0 Operational Policies	***Management/IT Support Personnel/General Users***	*Describes operational controls and procedures for securing County information and systems*
3.0 Technical Policies	***IT Support Personnel***	*Describes technical controls and specific security controls to secure County information and systems*
4.0 Acceptable Use	***All***	*Provides acceptable use and general use guidelines for users of County information technology systems and resources.*

1.0 MANAGEMENT POLICIES

1.1 Security Policy Program Management

Fairfax County shall authorize a Chief Cyber Security and Privacy Officer position with the mission and resources to coordinate, develop, implement and enforce a county-wide information security program. This position is appointed by the Chief Technology Officer, with approval by the County Executive.

The Chief Cyber Security and Privacy Officer shall develop formal information system security policies and procedures that address purpose, scope, roles and responsibilities, management commitment, coordination among agencies and departments, and operational and technical controls to ensure compliance consistent with applicable federal, state, and local laws, directives, policies, regulations, standards, and guidance. The security policy and procedures shall define minimum acceptable parameters for the implementation and use of information technology, communications systems and data (sometimes referred to as 'IT assets' and 'content'); authorized boundaries- technical and behavioral; provide an overview of security requirements for information systems, describe security controls in place for mitigating risk and achieving compliance, and be formally approved by authorized or delegated officials.

The Security Policy, procedures and related guidelines shall be periodically reviewed for effectiveness of security controls, roles and responsibilities, and, it shall be updated for industry, legal, legislative, or other technological changes. Changes and modifications shall be reviewed by the Chief Technology Officer and presented to the Senior IT Steering Committee for final adoption.

County developed information system security policies, procedures, and other guidance shall be published centrally located in the ISO and posted on the county's intranet readily available to all users.

1.2 Security Assessment and Authorization

The Information Security Office (ISO) shall develop formal and documented security assessment and authorization procedures and strategies that address purpose, scope, roles and responsibilities, management commitment, coordination among agencies and departments, and operational and technical controls to ensure compliance consistent with County policy, and applicable federal, state, and local laws, directives, operational policies, regulations, standards, and guidance.

The Chief Cyber Security and Privacy Officer shall annually review security assessment policies, procedures, and strategies and determine the effectiveness of existing security controls and team roles and responsibilities. ISO shall also produce analytical reports that detail the results of security assessments and implement plans of action to improve information security controls. Changes and modifications shall be reviewed by the CTO and presented to the Senior IT Steering Committee.
The CCSPO or Auditors may employ an independent assessment team to test and review security controls to ensure compliance consistent with applicable federal, state, and local laws, directives, policies, regulations, standards, and guidance.

County leadership shall determine personnel authorized to determine the acceptable levels of risk to County operations and information assets to guide the implementation of appropriate security controls. This includes (as deemed appropriate) Business Agency sponsor, CCSPO, Internal Auditor, County Attorney, CTO, Senior IT Steering Committee (or e-Gov Steering Committee), etc. Agency leadership and designated approval authorities are responsible and accountable for exercising due care in assessing the security risks associated with Fairfax County government information and systems and due diligence that the information security program and measures are implemented accordingly.

Agencies' leadership must formally authorize connections from County information systems to external information systems through interconnection security agreements such as Memoranda of Understandings (MOUs), Service Level Agreements, Firewall Rules Requests, Exceptions to Policy/Waivers, etc. Requests shall include details specific to each connection including the system or data source being connect to, the interface characteristics, security requirements, and type of information transmitted. Interconnections shall be monitored to verify enforcement of security use policy, controls and requirements.

ISO shall implement a continuous security program that allows County agencies to maintain security baselines adaptive to evolving threats, vulnerabilities, and technologies yet remain in alignment with County missions, goals, and values. The County Security program shall include a configuration management process, determinations of impact of changes to information systems and operations, monitoring, ongoing security control assessments, and reporting the security state of information systems.

1.3 Risk Assessment

The Chief Security Officer shall develop a risk assessment program that addresses the purpose, scope, roles and responsibilities, management commitment, technical controls and procedures, and adequate coordination among County agencies to ensure adequate security controls consistent with applicable federal, state, and local laws, directives, policies, regulations, standards, and guidance.

The Information Security Office (ISO) may initiate and/or conduct initial risk assessments for new County information systems to determine the likelihood and magnitude of harm in the event of unauthorized access, use, disclosure, disruption, modification, or destruction of County information systems and the information processed, stored, or transmitted. Project plans for new system shall include a risk assessment prior to final configuration. ISO may also perform and periodic assessments on certain existing systems, and/or compel the business/owner agency to do so.

Risk analyses and assessments of County information and systems shall include determination of values associated with critical infrastructure and other information system assets, the associated vulnerabilities and threats to the information and systems, the probability and impact of potential threats, and cost benefit comparisons of impacts and associated countermeasures.

The Information Security Office shall use vulnerability scanning tools to identify vulnerabilities that impact the confidentiality, integrity, and availability of County technology infrastructure, information and systems, and if found, compel remediation.

System owners should perform a Business Impact Analysis (BIA) and Risk Assessment (RA) on their application(s) or technology system. By this **Policy**, Agency heads are responsible for the security of the agency's information systems and therefore shall ensure the inclusion of BIA/RA for their agencies' essential systems in the County-wide Continuity of Operations Planning (COOP) efforts. Agency's IT Security Coordinator, System Administrator, business practitioner lead should conduct a BIA/RA throughout the agency to identify levels of sensitivity associated with data assets owned by the agency, potential security threats, and to determine the appropriate level of security to be implemented. Agency BIA/RAs should be performed in consultation and coordination with the Information Security Office.

1.4 System and Service Acquisition

Fairfax County systems and service acquisition process shall include language referring to the County's IT Security Policy, HIPAA Policy, and PCI-DSS Compliance as a requirement as applicable. As part of the technical acquisition process, Agencies shall ensure that a firm's submission includes a completed "Information Technology Security Policy Requirements Matrix for RFPs"" and be prepared to respond to queries for clarification from the Information Security Office, the RFP Technical Advisory Committee, or DIT Architecture Review Board.

County agencies' solicitation process to acquire IT products, solutions and services shall include a determination of information security requirements and should include clear delineation and understanding of roles and responsibilities of the vendor/contractor/solution provider and the county agency staff, reference to the County's IT Security, HIPAA and/or PCI-DSS Policies as applicable. In addition, Agencies should ensure that as part of the request for proposal process for IT products and services, a signed acknowledgement is received from the firm indicating their consent to the terms of acceptable use as defined in the Fairfax County IT Contractor/Consultant agreement form, the IT Security Policy, and/or any other policies or standards issued by Fairfax County.

Agencies are required to ensure adequate security controls are included in the solution, implementation process of the solution, and maintenance/support services consistent with applicable federal, state, and local laws and County policies, and, the project plan must indicate the required resources to protect the information systems as part of planning and investment, and include budgetary line items specific for implementing technical and operational security controls for information systems throughout the information system life cycle.

Agencies shall work with DIT and/or ISO in finalizing their solution requirements prior to solicitation, and for assistance with vendors, contractors, and other parties. Solutions shall include identification of the functional properties of information security controls to be employed, components, or services to permit the analysis and testing of those controls as required by County IT Security **Policy**. This includes the engagement of DIT and ISO divisions in regards to the acquisition and purchase of information technology products, services and devices, whether deployed in a vendor-hosted cloud or on-premises environment, hardware and software, and other related devices or systems requiring integration with Fairfax County enterprise architecture and systems, i.e. “Internet of Things”.

Software services vendors and manufacturers must demonstrate that acquired products, components, applications, and services employ the necessary security compliance standards, quality control processes, and validation techniques, and provide necessary documentation related to the use, configuration, installation, operation, and use and maintenance of security features and functions of an acquired product, component, or service. Services provider/implementers must adhere to implementing the standards in the solution required by Policy, or if not available, work with the ISO for a mitigating resolution or Waiver if necessary.

Providers of external information system services (hosted, WEB-based, or ‘Clouds’) must comply with County information security requirements and employ appropriate security controls in accordance with applicable federal, state, and local laws, orders, directives, policies, regulations, standards, and guidance. Contracts shall define County oversight, internal and external user roles and responsibilities, and processes to monitor security control compliance by external service providers.

The application of information system security engineering principles in the design, development, implementation, modification, and operation of County information systems integrated throughout the entire system development lifecycle (SDLC). The systems development lifecycle shall include the development of effective security policy, architecture, and controls as a foundation, define physical and logical boundaries, and incorporate security throughout the entire system lifecycle.

2.0 OPERATIONAL POLICIES

2.1 Awareness and Training

An information security awareness and training program shall be incorporated as part of the County's training and education programs for employees and others to educate the user community in the issues related to vulnerabilities and cyber-security breach risks associated with information technology, and the importance and methods of protecting County information and information systems. Security awareness shall be continually emphasized, reinforced, updated, and validated.

DIT and the ISO shall develop and maintain a communications process for notifying users of new information system security related issues and concerns specific to the County and of general interest.

New users of Fairfax County Government information systems shall attend or participate in an approved Information Technology and Information Security Awareness orientation training class **within 90 days** of being granted access to any Fairfax County information systems.

Users shall receive security awareness training and sign an acknowledgement indicating they have read Fairfax County information security policies. Records or certifications indicating the completion of security awareness training shall be retained for County users.

The information security policies, procedures, and other guidance are centrally managed and readily available via ISO to all users, administrators, and other stakeholders.

2.2 Configuration and Change Management

Changes to Fairfax County information systems and network architecture, such as operating systems, hardware, network devices, and applications are subject to the **DIT Change Management Policy Memorandum #9.**

IT systems shall be designed, configured, hardened, and maintained according to County System Hardening Standards to adequately safeguard County information to the extent possible or feasible. Baseline configurations and configuration deviations of Fairfax County information systems, network devices, and communications infrastructure shall be documented, reviewed, and updated. General requirements include, but are not limited to, installing operating systems from DIT-approved sources and media, applying vendor patches, removing or disabling unnecessary software and services, enabling audit logging and other security protections, and changing the passwords and usernames of default accounts. System owners are prohibited from making unauthorized changes to approved configurations without consultation and approval from DIT/ISO.

System Administrators shall analyze hardware and software for flaws, weaknesses, incompatibility, and other security or functionality impacts and vulnerabilities in a test environment prior to an implementation into the production environment. Security functions shall be reviewed and verified after changes to systems have been implemented to ensure the functions and features are implemented correctly, operating as intended, and producing the desired result.

Changes to Fairfax County information systems shall be implemented after a security impact analysis has been conducted to include a risk assessment and determination if additional security controls need to be implemented

ISO is a part of the Change Management process and shall enforce access restrictions to information systems to authorized personnel, and monitor information system changes to identify and deter unauthorized changes.

Mandatory configuration settings within the information system will be maintained using configuration baseline standards, and security configuration checklists that reflect the approved operational requirements. Exceptions from the mandatory configuration settings for systems, components, and services will be formally requested, documented, and approved by the Information Security Office. Information system configurations shall provide only the necessary capabilities by restricting the use of unnecessary functions, ports, protocols, and services.

An inventory of information system assets, components, software, and services in under DIT's custody shall be maintained. Agencies shall maintain a local inventory of assets under its control and periodically reassess the inventory. Information System Assets shall have identification numbers affixed in obvious locations as possible.

DIT shall be responsible for all aspects of the Fairfax County technology and communications infrastructure and will manage and administer all future developments, implementations, and enhancements to this infrastructure. This includes the data and voice networks, independent or converged, and their county-side interconnection devices to other networks. County network devices shall be configured to industry standard best practices and in compliance with County security policy and Hardening Standards.

Agencies are prohibited from making modifications, additions, and/or the removal of network management devices and configurations. If required, approval must be obtained through the Fairfax County Configuration and Change Management Procedures. Modifications and additions to network infrastructure shall be governed by a change management process.

Agencies must inform DIT of activity at their sites that include requiring a network or communications device or system to be removed. DIT may make any change deemed necessary as required in supporting the reliability and integrity of the IT infrastructure, to include protection from harms deemed through monitoring or as informed through ISO or law enforcement. Configurations for systems, software, hardware, infrastructure, and peripherals shall be formalized, documented, and periodically reviewed. DIT reserves the right to remove any network device that does not comply with standards or is considered to not be adequately secure.

2.3 Contingency Planning

Fairfax County Government IT infrastructure and critical information systems should have a viable Continuity of Operations Plan (COOP) and a Disaster Recovery Plan to continue an ability to function in the event of an IT emergency or interruption, and, to respond to and enable the restoration of vital operations and resources in a reasonable time.   DIT shall identify information systems processing and data storage plans which include alternative site(s) for essential systems that permit the restoration of information systems in the event of an interruption, failure, or compromise to the County’s primary processing site. A prioritization of critical system restoration for various situations should be included.

Fairfax County Government shall maintain contingency plans for County-owned information systems used for essential missions and business functions. Contingency plans shall include the identification of critical infrastructure systems and functions, provide restoration priorities and expected timeframes, address staff roles and responsibilities in the event of a disaster, consider alternatives to maintaining essential mission and business functions during an interruption, compromise, or failure and address the eventual information system restoration without deterioration of the security measures originally defined.   Options for contingency or mitigation for the agencies using externally hosted/ 3rd party provided solutions should also be addressed in contracts for those systems or expressly determined not essential by the owner agency.

Backups of identified user and system data essential to maintaining operations shall be identified and protected at an offsite location. Physical and technical measures to ensure the recovery of information systems to a known state after a disruption, compromise, or failure shall be maintained. Measures may include securing copies of operating systems, software, and firmware installations or configurations on physical media or at a commercial off-site location; and maintaining backups of user, system, and configuration data for information systems and network infrastructure.

Fairfax County government should design network and telecommunications that minimizes wholesale network disruptions and establish alternate back-up services to resume information system operations for essential mission and business functions when the primary network/telecommunications capabilities are unavailable.

Agency management shall determine the necessity and acceptable risk for their systems and ensure the necessary allocation of personnel and resources for the development and maintenance of a COOP for critical information systems supporting of essential business functions.   DIT will consult with agency personnel responsible for developing agency-specific COOP and conducting business impact analyses for essential information systems. Contingency plans should be reviewed and tested to determine effectiveness and readiness. Exercise results shall be documented, and any corrective actions shall be initiated upon discovery.

2.4 Incident Management and Response

ISO shall develop, disseminate, and periodically review and update a formally approved incident response procedure that addresses the purpose, scope, roles and responsibilities, coordination among internal and external agencies or entities, operational and technical controls, and processes and procedures to implement an incident response policy and associated incident response controls that is effective and consistent with enterprise and operational architecture.

A Computer Incident Response Team (CIRT) shall be established by the CCSPO in the event of a security incident, such as a virus, worm, hoax email, theft of a County-owned information asset, detection or discovery of unauthorized devices, detection or discovery of hacking or hacking tools, altered data, misuse of information systems as defined in **Acceptable Use policy**, or other suspected or confirmed event.   CIRT members shall have pre-defined roles and responsibilities which can take priority over normal operational support duties.

CIRT personnel shall be responsible for ensuring any damage or vulnerabilities to County information systems due to an incident are repaired, mitigated, eliminated, or minimized.

CIRT personnel shall be responsible for communicating and coordinating with vendors and manufacturers concerning the identification of discovered malware and vulnerabilities on County systems and working with vendors and manufacturers towards eliminating or mitigating any discovered vulnerabilities.

Incident response procedures for security incidents shall include the preparation, detection and analysis, containment, eradication, and recovery of County information systems. Incident response procedures shall be consistent with contingency planning activities. Security incidents shall be tracked and documented to include identifiable information unique to each incident, incident status, and any supportive forensic evidence. The CCSPO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT and determining any physical and electronic evidence to be acquired as part of the investigation.

The CCSPO is responsible for reporting and coordinating communication related to an information security incident to the Department of Human Resources and other federal, state, or local law enforcement authorities as required.

The CTO and CCSPO shall determine if widespread Fairfax County communication is required in the event of a security incident, to include the content of the communication and best distribution method.

Exercises should be periodically conducted to determine the effectiveness of incident response capabilities, processes, and procedures, document the results of these exercises, and update incident management and response policies and procedures as necessary to improve capabilities.

2.5 Collection, Retention, and Classification of Electronic Data

Fairfax County information systems contain electronic/digital data and information – "data". Any data within any Fairfax County information or communications systems, (i.e. all Fairfax County departments, agencies or interconnected partner entities) is the property of Fairfax County. Fairfax County Agencies are responsible for ensuring compliance with all current or future Federal regulations and laws(HIPAA, PCI, PII), the Virginia Public Records Act and Records Management Retention and Disposition Schedules issued by the Library of Virginia (LVA), and any other laws, regulations, mandate, or guidelines of the Commonwealth of Virginia; all Fairfax County regulations, policies and any other applicable guidelines to the data type of electronic records processed by the Agency. The Fairfax County Board of Supervisors, the County Executive or Agency Heads may elect to supplement and provide additional policy or guidance related to data classification, use, retention, release, and destruction.

Guidance on records retention under the Virginia Public Records Act can be found at Virginia Public Records Management Manual. Employees, contractors, partners, and any person that have access and use County information systems and data must comply with the retention of records requirements and must categorize records appropriately to ensure the appropriate disposition of specified records at the end of the applicable scheduled retention period.

Agencies are the experts and stewards of the information and data within their designated mission and requisite responsibility, systems and processes, thus classified in the IT Security Policy as 'Data Owner'. Data Owner, or other designated Agency personnel, shall be responsible for determining the data classification levels for information processed on County information systems, and when such data is in hard copy form. Agency Heads are responsible for the ultimate management and compliance of data classification for their agency, based on County policy, executive and/or legislative authorization. Classification levels shall be documented and mapped to data protection measures.

DIT is responsible for developing and maintaining enterprise information architecture and standards. See page 13 of the Guiding Principles section for details regarding information classification types.

Data owners shall ensure that systems have been implemented with the appropriate security controls before any Confidential or Sensitive data is processed on systems.

Owners of Confidential or Sensitive data shall ensure that users receive training in the protection requirements for securing information. Data owners may choose to require the authorized user's signature to acknowledge this notification.

Information stored electronically or on paper shall be evaluated for criticality and sensitivity. The criticality of data shall identify the degree to which the organization depends on the data for continued operations or even survival. ISO will provide guidance in regard to data protection standards regardless of information medium, to include but not limited to, electronic storage and transmission, film, or paper.

Physical marking, labeling, or other notation is required to identify all documents, email, media, or reproductions of confidential information. Information not specifically labeled will be treated as Internal Use information.

Collections of information from various sources with multiple classifications shall be classified at the highest sensitivity level of the information included.

The sale or release of County information to external individuals or organizations, such as email distribution lists and departmental telephone directories, shall comply with County legal and fiscal policies and procedures.

Authorized personnel to publish information to County information systems and applications that are publicly accessible shall be designated. The County's e-Government Steering Committee, which includes a Deputy County Executive – executive sponsor, the Office of Public Affairs Director, CCSPO, CTO, County Attorney, and e-Gov director determine the process for properly classified information publishing on electronic venues such as the County Website, and Social Media resources.

Authorized personnel shall ensure that publicly accessible information does not contain non-public information such as information protected by law. Authorized personnel shall review all content proposed to be published to a publicly accessible information system prior to release.

Sensitive or Confidential information may not be removed on media from Fairfax County Government premises unless the information owner has approved in advance. Media may include, but is not limited to, external hard drives, flash drives, floppy disks, CDs, DVDs, magnetic tape cartridges, and paper documents.

Data owners shall ensure that security measures are implemented prior to the transmission of County Confidential or Sensitive information to destination systems and that destination systems are adequately secured according to the adequate protection requirements.

2.6 System and Data Security Maintenance

The confidentiality, integrity, and availability of County information are sustained through information system maintenance policies and procedures for systems installed on-site, at remote sites, or through remote third-party processes.

Maintenance procedures should be documented. Maintenance records should be kept and include the date and time of maintenance, name of individual performing maintenance, a description of maintenance performed, and a list of any equipment removed or replaced. A log of any persons requiring escort that are not pre-authorized/badged is required if access is needed in a secure facility.

System functionality, security controls, and approved baselines must be tested and validated after maintenance or repair.

Maintenance agreements through County contracts shall include reference to the County IT Security policy. When spare parts equipment maintenance is required, system owners must explicitly approve the removal of any devices or formats from County information systems requiring maintenance. Hard drives, storage media and other devices shall be sanitized prior to removal from County facilities and prior to the release to vendors or maintenance personnel for maintenance to prevent unauthorized disclosure of data and minimize impacts to the confidentiality, integrity and availability of County information systems and data. Any diagnostic tool used may be inspected and/or will be scanned for malicious code prior to introduction to County systems.

Maintenance personnel, to include manufacturers, contractors, vendors, and other personnel, shall hold formal access authorization from designated County personnel to conduct maintenance on County information systems, components, and software. Personnel authorized to escort maintenance personnel shall have the necessary technical competence to supervise information systems maintenance.

2.7 Media Protection

Information systems, diagnostic tools and applications, and data storage devices must be approved for use to access Fairfax County systems and information. Information systems and devices may not be connected to the Fairfax County network infrastructure unless accredited and approved by DIT. Any personally owned devices such as music players, PDAs, memory devices, USB drives or similar, smart phones, tablets, and cameras are prohibited from being connected to County-owned resources unless authorized through a formal approval process. These devices if approved for use will be connected to county mobile device management system, and use may be monitored by DIT. If found outside IT Security compliance guidelines DIT is authorized confiscate the device and write a security violation.

Agencies shall maintain record of media of storage media that contains County information during transit outside of County controlled areas and facilities.

County usage of approved mobile communications devices to access County information, regardless of whether connected to County networks or carrier provider networks, is subject to County standards, policies, and procedures.

Fairfax County Government information systems and storage devices shall be acquired by Fairfax County and registered to DIT. Device identification shall include the IT Resource contact name and location, a backup contact, the hardware and operating system platform and version, and the main business functions and applications. **Devices provided by partners and/or through grants that may be acquired by other parties are subject to this policy**.

County information stored on decommissioned hardware and storage media shall be irretrievably destroyed, in a manner to permanently and irreversibly delete data to prevent access by unauthorized individuals. Storage media may include, but is not limited to, hard drives, storage systems, removable disks, floppy disks, CDs, flash drives, and other forms of removable media and storage devices. Sanitization requirements will be determined by the system profile of the device to be decommissioned and the sensitivity level of the information processed or stored.

Agencies shall use an approved media erasing tool to ensure with reasonable expectation that information is overwritten on County information systems, electronic media, and storage devices prior to disposal or reuse. Agencies shall utilize sanitization methods with the strength and integrity commensurate with the classification or sensitivity of the information.

Storage media and devices shall be sanitized prior to the release to vendors or maintenance personnel for maintenance to prevent unauthorized disclosure of data.

Fairfax County Government agencies shall maintain control and record of the transit of storage media that contains County information outside of County controlled areas and facilities.

2.8 User Security

DIT gives access to the County's IT enterprise/network log-on. Agency system owners grant access to their applications, following IT Security Policy and practices.

Access to County information and systems shall only be granted to authorized users who include all employees – merit or non-merit, technical support or end-users, authorized contractors, and volunteers with a valid access need to perform official County duties.

County employees and contractors that are authorized to perform privileged user functions, such as developing, implementing and/or administering County information systems, shall sign and acknowledge the requirements of acceptable use and privileged use. Agencies should have County employees and contractors sign agreements defining the acceptable use of information systems and information protection requirements to assist in deterring the unauthorized disclosure of County Confidential, Sensitive, and Internal Use information and mitigating risk to County information systems. A copy of **Agreements will be kept by ISO**. ISO has a standard Agreement for IT Consultants that may be used. This agreement must be included in county RFPs and/or contracts whereby contractors will be used to develop IT systems and/or data.

Legal and contractual prerequisites such as background checks and non-disclosure agreements should be completed prior to access being granted to County information or systems. ISO may refuse access when proof of background check is not disclosed. Companies with a county contract are ultimately responsible that their contractors assigned have met the background check requirements, and associated management official of the company signs the form on the companies' behalf.

County employees or contractors separating or terminating employment with Fairfax County Government shall have access to information systems and information revoked and the Employee Clearance Record must be completed (HR Procedural Memorandum #33). Additional measures may include, but are not limited to, removing users from access lists, changing or reprogramming combinations or access card systems and passcodes, and informing outside agencies of personnel changes. Volunteers, service providers, vendors or other personnel granted access to County systems shall have all access revoked once no longer needed.

Fairfax County shall recover and retain all access to information and systems controlled by former employees or contractors. Separating County employees and contractors shall return all property owned by Fairfax County Government including, but not limited to, systems, software, equipment, devices, media, access badges and tokens, mobile devices and telephones, physical keys, hard and soft copy documents, and other information and materials.

Agencies designated staff with either management, AISC, or AACA role shall review logical and physical access authorizations to information systems and facilities for reassigned or transferred employees still employed with Fairfax County Government. System access and privileges shall be updated and modified according to the principle of least privilege.

Fairfax County shall enforce and document the allocation of distinct information system duties (roles) for employees and contractors into separate job functions performed by different individuals through assigned information system authorizations. Separation of duties (SOD) shall be incorporated into Change Management processes and procedures.

Users shall not have the authority or ability to circumvent technical or operational security policy for systems storing County information in which the assurance of integrity, access control, or confidentiality is required. Any attempt to circumvent controls is considered a Security Policy violation.

Fairfax County has a formal sanctions process for personnel failing to comply with approved information security policies and procedures, and acceptable use policies. The sanctions process shall be consistent with applicable federal, state, and local laws, orders, directives, policies, regulations, standards, and guidance. ISO is authorized to initiate the process.

2.8.1 Third Party Access

Third parties to include vendors, contractors, other governmental partners, and volunteers as system 'users', either on premise or remote, shall comply with all applicable federal, state, and local policies, practices, standards and agreements, including, but not limited to safety, privacy, information security, conduct, and acceptable use if given access to Fairfax County information systems, information and data as indicated in section 2.7 above.

Fairfax County shall retain all proprietary rights to the content in its information systems, code developed by a third party for Fairfax County, and system and program data requirements for computer systems security. In services provided by third parties such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), remote data storage, etc., the third party is responsible to maintain Fairfax County processes, information and data per the Fairfax County IT Security Policy, or better. This includes unauthorized use and disclosure of data and information intended or unintended the service and its personnel support.

Access to County information with special protection requirements shall only be granted to County contractors with valid access needs as assigned to perform duties. Vendor personnel security requirements shall include defined security roles and personnel security requirements for employment.

Third party agreements and contracts shall identify the Fairfax County information to which the third party should have access and state the third-party responsibilities in protecting that information. Agreements and contracts should also define the acceptable methods for the return, destruction, or disposal of Fairfax County information in a third party's possession at the termination of the contract as in Section 2.7 above.

Third parties shall only use Fairfax County information and systems for the purpose of the business agreement and any other Fairfax County information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others. Unless allowed in the contract, a third party may not give access to or distribute Fairfax County systems, information and data to another third party without permission by Fairfax County.

Compliance with contracts and third-party agreements shall be monitored.

Third parties shall provide the Fairfax County contracting agent and sponsor agency with a list of its employees working on the contract that need access to Fairfax County systems and data. The list shall be updated and provided to Fairfax County within 24 hours of staff changes. Sponsoring agencies shall provide the list to ISO. In the case of 'Cloud' services whereby the firms' employees have aggregated responsibility for carrying out the contracted services with no specifically named individuals for the contract, the firm accepts all responsibility.

Third parties with access to Fairfax County Confidential and Sensitive information shall have the appropriate clearance to handle that information. Third parties will ensure that all Confidential or Sensitive information is collected and returned to Fairfax County or destroyed within 24 hours in the event of a separation or termination of third-party employment.

Third party vendor accounts and maintenance equipment on the Fairfax County network that connects to the Internet, telephone lines, or leased lines shall be disabled when not in use for authorized maintenance or support.

Third party accounts shall uniquely identify the user and passwords shall comply with the Fairfax County Password Policy and Administrator/Special Access Policy, or better. Third party work activities shall be tracked in a maintenance log and available to Fairfax County management upon request. Logs shall include as appropriate, but are not limited to, events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

Third parties are required to comply with all federal, state and Fairfax County auditing requirements, including the auditing of the third party's work.

Software and hardware used by third parties providing services to Fairfax County shall be properly inventoried and licensed.

Contractors found to be in violation of County policies will have their systems access revoked, devices confiscated, and may also be removed from the Fairfax County engagement.

2.9 Privileged Administrative Access

Administrative or privileged access may be defined as maintaining advanced privileges or system access as opposed to those of the general user community. Employees and contractors that are authorized to perform privileged user functions, such as administering County information systems, developing systems, applications, databases, websites, interfaces, conducting maintenance and 'break fix' support activities, etc., shall sign and acknowledge the requirements of acceptable use and conditions of privileged use as defined in the **Administrative/Special Use Agreement Form**.

Administrative users shall also be provided a separate general user account in accordance with this policy to perform normal business functions.

Privileged administrative access accounts needed for internal or external audits, investigations, software development, software installations or other defined needs, shall be authorized by the CCSPO, created with an expiration date, and disabled when no longer needed.

Agencies shall maintain a centralized list of their administrative/privileged users for any County information systems. Personnel granted privileged administrative access shall be issued a unique administrator account. Administrative users shall maintain and follow administrative account management instructions and documentation. Administrator accounts shall only be used to complete assigned duties that require advanced privileges. Accounts used for administrative or privileged access shall meet the Fairfax County password complexity requirements defined in this policy.

Shared access or group administrative accounts must be approved through the Exception Request Process.

System accounts should be configured to follow the concept of least privilege and not maintain open excessive privileges for the sake of convenience. System accounts that require administrative privileges must also be formally documented and approved by the ISO.

Inactive privileged system accounts or privileged user accounts shall be reviewed and disabled according to County policy. ISO is authorized to force-through disabling an account on any county system.

Administrative users shall not misuse their administrative privileges, and specifically not use their privileges to circumvent security policy. ISO has the right to monitor use; any violation of policy noticed or reported will result in investigation and/or county HR policy sanctions.

A password escrow procedure should be implemented to allow administrative access to the system during an emergency.

2.10 Physical and Environmental Protection

Facilities that host critical information system should be a secure environment with access restricted to authorized personnel. The Department of Facilities Management (FMD) Security Office works with ISO in authorizing physical access to restricted IT facilities. Access to information systems facilities may be further restricted by the CCSPO upon actual or potential security threats, events, or circumstances. Signage for restricted access areas and locations shall be practical and clear but the importance of the location shall be minimally discernible.

Access to information systems facilities shall be granted only to Fairfax County employees and contractors whose job responsibilities require access to that facility through controlling mechanisms. Access control options may include sign-in, badge, electronic keys, cameras, and other mechanisms with auditable access logs and tracking. Access requests to information system facilities shall be approved by applicable Fairfax County system and data owners and may include the approval of agency county staff responsible for the facility and DIT as applicable.

Employees and contractors authorized access shall be documented, tracked and reassessed periodically. FMD conducts monitoring and auditing physical access to information systems restricted facilities. Agencies shall update their list of authorized users give system access. ISO will work with agencies and/or FMD in reviewing physical access requirements for employees and contractors.

On-site vendor employees/contractors that require access to County systems shall always be credentialed - acquire a Fairfax County identification badge to be displayed while on the Fairfax County premises. The credentials are property of Fairfax County and shall be returned to Fairfax County when the employee leaves the contract or at the completion of the contract. Upon contract termination or at the request of Fairfax County, third parties shall surrender all Fairfax County identification badges, access cards, data, equipment, and supplies immediately.

Access cards, keys and/or other credentials to information system facilities shall not be shared or loaned to others. Access cards and keys that are no longer needed shall be returned to the facility access control administrator. Cards shall not be reassigned to another individual bypassing the return process. Lost or stolen access cards and keys shall be reported to FMD and the agency responsible for the information systems facility. Signature cards held by off-site backup storage vendors for access to Fairfax County backup media shall be reviewed annually or when an authorized individual leaves Fairfax County.

Access cards and keys to information systems facilities shall not be labeled with descriptive information that identifies the facility location. Cards and keys may display a return mail address in the event the card or key is lost and then found.

Physical access controls implemented at off-site backup storage locations shall meet or exceed the physical access controls of the source systems. Additionally, backup media shall be protected in accordance with the highest Fairfax County sensitivity level of information stored.

Agreements and procedures between Fairfax County and off-site backup storage vendors shall be reviewed annually and updated as required.

Information system facilities that allow visitor access may require a sign in/out log in addition to the system access logs. Card access records and visitor logs for all information systems facilities shall be archived. Information system facility access control administrators shall review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Visitors shall be escorted in restricted areas of information system facilities. Individuals granted unescorted access to an information systems facility shall sign any required facility access agreements.

County personnel responsible for information systems facilities shall alert the FMD Security Office and/or ISO to remove the access privileges of individuals whose role(s) change.

Physical access to information system infrastructure, distribution and transmission lines within County facilities shall be controlled to assist as a preventive measure to accidental damage, disruption, and physical tampering. Emergency power shutoff capabilities shall be protected from unauthorized or unrestrained activation.

Operational and technical controls of information system output devices shall be implemented to protect information from unauthorized access. Physical operation controls to protect output devices may include not placing printers, copiers, and fax machines in open public areas, and removing printer or copier device storage prior to external maintenance particularly related to output that contains sensitive information. Examples of technical controls may include enabling screen savers, using monitor screens, card access controls, user-ID and passwords.

Passwords should be established on county issued PDAs, Smartphones, and tablets, especially when the device is used for accessing or imputing sensitive data, through email or system of record databases.

When personally owned devices are approved and configured by DIT for use accessing County systems and data, the device and use are subject to this **Policy**. Employees using personally owned devices will sign a security agreement form for this purpose.

2.11 Software Licensing and Usage

Commercial software that has not been acquired through official county procurement process or channels is prohibited and cannot be installed on any county system to include websites. Copyrighted software for which Fairfax County does not have specific approval to use shall not be installed or stored on Fairfax County information systems. Systems administrators will remove any software determined to be unlicensed or unapproved.

General users, as opposed to privileged users, will not be allowed to install software and applications unless given a Waiver and/or express permission by ISO.

Users should not download software products or unauthorized open source from the Internet without approval from the agencies' system administrator, unless it is required to view/receive/read documents and information from that source that includes a step to allow the download.

Software used by Fairfax County shall not be duplicated unless usage is consistent with relevant license agreements, prior management approval has been obtained, or copies are being archived for contingency planning purposes and/or software escrow agreements/contracts.

County employees and contractors shall abide by all software and product license agreements and not illegally copy or distribute software. DIT is authorized to remove any unlicensed or unapproved software from any County information system. ISO may initiate an investigation when illegal or unauthorized software is found on county systems.

2.12 Supply Chain Protection

County IT and IT Security policies and standards shall be applied for information systems, components, and products whereby they do not violate license agreements and warranties. ISO may conduct review of contractual agreements that involve IT products/services supply chain process for integrity and vulnerability assessment that may compromise its use.

Fairfax County systems shall be designed, configured, and maintained according to County System Hardening Standards to adequately safeguard County information.
It is expected that hosted, software-as-a service and 'cloud' solutions have followed industry standards and due care in providing systems, and that service level agreements and warranties are expressed in contracts to the level of the county's IT Security Policy.

All firms, vendors, contractors, consultants either supplying IT and communications products to Fairfax County or supplying staff resources (contractors/consultants) are required to adhere to Fairfax County IT Security Policies, and for contractors, will be required to sign the **ISO Contractor Agreement** form. Any firm's consultants or contractors engaged who violate county policies will be exited from the county and contract.

The security architecture of software applications acquired through the procurement process will be taken into consideration in the evaluation process and selection. If the product deviates from county IT security or architecture standards but is best business fit as determined through the selection process, an ISO Waiver is required.

Language regarding requirement for products and services to adhere to privacy policies to include HIPAA, PCI, PII and others must be included in solicitation documents and may not be negotiated out or deleted from contracts where required.

2.13 System and Information Integrity

IT Systems and data must be protected from unauthorized use, hacking, malicious activity that may interrupt services, compromise data.

IT System administrators and managers are required to assist in enforcing compliance for IT protection. Upon detection or notification from ISO or their system vendor for vulnerabilities or direct actions resulting from inappropriate use in their agency, it is expected that immediate action to remediate the issue is conducted by them or ISO directly. ISO may remove any devices or disable unauthorized products without notice.

Operational and technical controls to protect against malicious code at information system gateways and endpoints of shall be implemented. Malicious code protection mechanisms are to be updated automatically as available.

Agencies that administer systems directly are required to follow this policy. When found in violation, ISO will inform the agency of a violation of policy. If through the agency's negligence in patching vulnerabilities damage is caused to the county IT enterprise, the agencies will be responsible for the cost of mitigation and repair.

Fairfax County will utilize operational and technical controls to detect system attacks and identify unauthorized use of County information systems. Tools shall be employed that support near real-time analysis of events, monitor inbound and outbound communication with provisions for inspecting encrypted traffic, automatically alert security personnel at an indication of compromise, and prevent users from circumventing detection capabilities. **All persons are prohibited from installing any capability that is designed to hack or compromise Fairfax County technology systems and assets.**

Data Loss Prevention (DLP) technologies shall be utilized and centrally managed to protect and minimize the disclosure of County Confidential and Sensitive data in transit and at rest.

System and security event correlation tools shall be utilized to achieve enterprise-wide situational awareness.

Delegated personnel shall receive information system security alerts, advisories, and directives from vendors, approved vulnerability advisory councils, and other organizations on a reoccurring basis. Security alerts, advisories, and directives shall be disseminated to personnel responsible for administering information systems and a timeframe shall be determined for implementation within the approved Configuration and Change Management process.

Integrity verification applications and tools shall be employed by ISO to inspect information for tampering, errors, and omissions. Operational policies and technical implementations shall be utilized to monitor the integrity of County information system and applications.

Spam protection mechanisms shall be deployed by ISO at information system gateways and on County information systems to detect unsolicited and potentially malicious messages and attachments.

Agencies are not allowed to independently deploy unauthorized IT security tools without permission of ISO.

2.14 Vulnerability Management

Vulnerability management is the process to identify, assess, and remediate Information Technology (IT) vulnerabilities, weaknesses, or exposures which can threaten the confidentiality, integrity, and availability of assets. Security vulnerabilities are inherent in information system operating systems, applications, firmware, and configurations. Software updates and patches are made available by manufacturers to remove security vulnerabilities, correct coding misconfigurations that cause unexpected operational results, or add new functionality. Unpatched systems may expose County systems and information to unauthorized access and disclosure and allow the propagation of malicious code which could disrupt County operations thus compromising the confidentiality, integrity and availability of County systems and information.

This shall apply to all existing and future implementations of information systems at Fairfax County Government. Any person or entity within or affiliated with Fairfax County managing an IT System that processes, stores, transmits, and/or collects Fairfax County data is responsible for complying with this policy. This policy is applicable to vendors and/or third parties providing hosted services or supporting traditional on-premises technology deployments. Failure to comply with the Fairfax County vulnerability management policy may result in the interruption of network service of the offending assets.

The Fairfax County Information Security Office (ISO) shall perform, at a minimum, quarterly discovery scans to identify assets that are not registered or inventoried, quarterly vulnerability scans on all information systems including, but not limited to, perimeter, data center, and workstation assets, and ad hoc vulnerability scans shall be performed at the ISO’s discretion in response to new server deployment, public facing firewall change requests, new threat intel, and system owner requests.

Vulnerabilities identified from scanning activities will be provided to the appropriate Department of Information Technology (DIT) and Agency/Agency Information Security Coordinator (AISC) point of contacts responsible for remediation efforts. A Plan of Action and Milestones (POAMs) document must be submitted to the ISO for vulnerabilities that cannot be remediated within remediation timeframes.

Vulnerability Remediation Timeframe Matrix

	Critical Vulnerabilities	High Vulnerabilities	Medium/Low Vulnerabilities
Perimeter/Payment Card Industry (PCI)	**7 Days**	**7 Days**	**7 Days**
Core Enterprise Resources: Active Directory, Domain Name System, Dynamic Host Configuration Protocol (DHCP), Multi-Agency File Servers/ Application Servers, System Center Configuration Management (SCCM)	**7 Days**	**7 Days**	**7 Days**
Desktop Workstations	**14 Days**	**14 Days**	**30 Days**
Mobile Devices	**14 Days**	**14 Days**	**30 Days**
Other	**14 Days**	**14 Days**	**30 Days**

Note: Deadlines as defined above apply to all systems, including systems previously approved for the installation of manual updates.

The following roles and responsibilities have been defined to ensure adherence to Fairfax County's Vulnerability Management plan.

Department of Information Technology (DIT)

DIT shall perform the following functions as part of the Fairfax County Government Vulnerability Management Strategy:

- Maintain a current inventory of hardware, software, operating systems, and applications used within the enterprise.
- Oversee the DIT Patch Management Strategy for deploying system patches and updates which will be measured and monitored for the following:
  - Microsoft Operating Systems and Applications
  - Anti-virus definitions and scan engines
  - Third Party applications (Adobe, Java, Foxit, etc.)
  - Hardware firmware
  - Non-Windows operating systems
- Review and remediate enterprise vulnerabilities identified via vulnerability scan results provided by the ISO.

Information Security Office (ISO)

ISO shall perform the following functions as part of the Fairfax County Government Vulnerability Management Strategy:

- Monitor for notifications of newly discovered vulnerabilities in operating systems, applications, and firmware.
- Perform vulnerability scanning of Fairfax County assets.

- Prioritize the order in which the County addresses remediating vulnerabilities based upon quantity of systems of affected, level of risk, likelihood of exploitation, and potential impact on operations.
- Verify vulnerability remediation through network and host vulnerability scanning.
- Review and request updates for POAMs submitted for vulnerabilities that cannot be remediated within remediation timeframes.

Agency/Agency Information Security Coordinator (AISC)

AISCs shall perform the following functions as part of the Fairfax County Government Vulnerability Management Strategy:

- Review agency vulnerability scan results provided by the ISO.
- Remediate or coordinate the remediation of agency assigned vulnerabilities.
- Ensure Agency system and application administrators are monitoring and proactively applying relevant system patches as released.
- Complete and submit vulnerability remediation extension requests to the ISO for vulnerabilities that cannot be remediated within the remediation timeframes.

The Fairfax County Chief Cyber Security and Privacy Officer and IT Security Program Director are authorized to institute any necessary measures to enforce and manage the compliance of County information systems. This may include powering off or disconnecting systems that introduce unacceptable risks and vulnerabilities to County assets. Plans of action for remediating vulnerabilities due to excessive missing patches and updates may be developed in coordination with the DIT Information Security Office.

There are no exceptions to the Fairfax County Vulnerability Management policy. If identified vulnerabilities cannot be remediated within the indicated timeframes, a POAM document must be submitted to the ISO for approval. Please contact infosec@fairfaxcounty.gov for more information.

2.15 System Development

County information systems shall be developed and maintained in accordance with the Systems Development Life Cycle, utilizing the Systems Development Life Cycle Standards (SDLCS) or similar. IT Security is a component of SLDCS.

Solutions must be coordinated with DIT before final acquisition and installation at Fairfax County. Information system security engineering standards and principles shall be incorporated in the design, development, implementation, modification, and operation of County information systems. The systems development lifecycle shall include the development of effective security policy, architecture, and controls as a foundation, defining physical and logical boundaries.

County information systems shall be managed by approved configuration and change management principles throughout the design, development, implementation, and operations of information systems. County agencies and data owners shall perform periodic risk assessments of systems to determine whether the controls employed are adequately mitigating the associated security risks.

Systems shall maintain access control features to restrict access in accordance with the concept of least privilege.

Application-program-based access paths other than the formal user access paths shall be deleted or disabled before software is moved into production.

Systems and resources used for development, testing, training and other similar purposes shall maintain separation from systems and resources used in the production environment.   Data released for testing, research, training and other similar purposes shall be sanitized prior to release to testers unless each individual has approved access to the information.

Risk assessments must be performed on systems as a part of the development process and system operations to ensure the confidentiality and integrity of systems, associated programs and data files.

To ensure proper segregation of duties, owner responsibilities shall not be delegated to the custodian.

3.0 TECHNICAL POLICIES

3.1 Audit and Accountability

Fairfax County information systems are subject to monitoring and relevant event log information shall be collected, correlated, and archived as evidence for investigations into potential malicious activity, misuse, information disclosure, and system anomalies.

Information systems shall have the appropriate hardware, software, configurations, or manual auditing mechanisms to log and archive relevant system, application, and security events when technically possible.

County information systems shall generate audit trail records that contain sufficient information to determine the type of event, date and time of event, location and affected systems, the source and destinations of an event, the success or failure of the event, and the identities of any users or objects associated with the event.

Audit log trails of significant events shall be maintained and archived for compliance with retention requirements. Exception reports (authentication, intrusion detection, etc.) shall be obtained and reviewed on a regular basis and as needed. Logs shall, at a minimum, capture the information needed to satisfy audit guidelines requested by Fairfax County Government internal and external auditors.

Agencies/application owners shall implement information system auditing procedures for auditing the system, review frequency, event reporting methods, retention periods for system event log data, and periodic testing the restoration of archived event log data.

Applications and systems with Confidential or Sensitive data shall log all local and remote access. Records shall identify user identities, time and date of access, medium of access request (local console, network, and dial-up), data being accessed, duration of connection, and protocol or application being accessed.

Audit log records for systems containing Confidential or Sensitive information shall be archived in a central repository, not on the local system (i.e., separate and secure server) for the timeframe defined by retention requirements.   Audit logs shall be irretrievably destroyed at the conclusion of the defined retention period.

System administrators and data owners shall review event logs on a periodic basis to detect unauthorized access attempts, unauthorized system changes, performance anomalies, and other events.

Changes to agency information systems, software, technical infrastructure, and system policy may be audited for integrity of access privileges and controls. Appropriate personnel shall be alerted in the event of system audit processing failures or the failure in collection of auditable events from County information systems. Audit failures must be mitigated unless a valid business justification or decision is made, or Waiver is given. If the issue is outside of the county's control, then the enterprise mitigation controls will carry the issue.

Fairfax County shall allocate the adequate storage capacity for collecting and maintaining records of auditable events and configure auditing to reduce the likelihood of such capacity being exceeded. Storage capacities and auditing configurations must still assist in ensuring compliance with records retention requirements, as well as ensuring the collection of relevant information system auditable events to conduct investigations into security incidents.

County information systems and network devices shall maintain centralized time synchronization with an approved time source server to ensure the generation of consistent time stamps across auditable event data.

Access to auditable security related event data shall be limited to authorized personnel and protected through methods such as encryption and system backup to ensure the confidentiality, integrity, and availability of auditable events.

3.2 Backup and Contingency

Part of IT Security management includes having appropriate processes for backing-up data, assuring the integrity of systems functionality, and maintaining operations.

Fairfax County Agencies are responsible for ensuring compliance with all current or future Federal regulations and laws (HIPAA, PCI, PII), the Virginia Public Records Act and Records Management Retention and Disposition Schedules issued by the Library of Virginia (LVA), and any other laws, regulations, mandate, or guidelines of the Commonwealth of Virginia; all Fairfax County regulations, policies and any other applicable guidelines to the data type of electronic records processed by the Agency. If necessary, Agencies shall communicate and coordinate any unique requirements with DIT in the event a technology solution is required to meet compliance. In some instances, Agencies are responsible for maintaining backups for data maintained within the agency and are not directly supported by DIT.   Backup frequency, retention, and destruction shall be in accordance with information classification levels, availability requirements specified by the data owner, and any legal and regulatory retention requirements such as defined above.

The data back-up process must use secure transport to ensure the integrity of the data. Backups of County Confidential and Sensitive information that is stored at vendor off-site storage facilities shall be encrypted.

Agencies shall maintain appropriate backup, contingency and continuity of business plans for recovery of systems in the event of a disaster based on agencies' risk assessments and business requirements.

Backup and recovery processes shall be documented, tested, and periodically reviewed.

Vendors that provide off-site storage services for Fairfax County backup archives shall have the appropriate clearance to handle the highest level of information stored.

3.3 Encryption

Encryption mechanisms shall be applied to information in transit across information systems, network infrastructure, and other communications architecture and data at rest on computer readable media when technically feasible to protect the confidentiality and integrity of County information.

Encryption usage requirements shall consider the type and classification level of information, laws that govern protection requirements, storage location or media type, transmission medium, and Fairfax County's internal requirements for the timely and continued availability of information.

Agencies shall establish standards and procedures that address when encryption, digital signatures, and digital certificates shall be used in accordance with Federal, State, and local laws, as well as County policies and guidance.

Agencies shall use open-standard based encryption algorithms to share encrypted data internally and externally for data that requires encryption to support interoperability needs.

Confidential or Sensitive data shall be encrypted during transmission using encryption measures strong enough to minimize the risk of the unauthorized disclosure if intercepted or misrouted.

Secure transmission methods shall be used to distribute decryption capabilities to the recipients of encrypted data. Options may include a public key infrastructure or a separate communication that includes a verification of the identity of the recipient.

Unencrypted copies of encrypted information shall be stored in a known location on County systems and encrypted information shall be available to more than one individual. Software and decryption keys may be stored using an appropriate digital escrow method.

Agency implementations of storage or transmission encryption shall include an encryption key management plan to protect the confidentiality, integrity, and availability of County information.

Encryption key management plans shall ensure that data can be decrypted in the event of loss or unavailability of cryptographic keys.

Encryption key management plans shall address the handling of keys suspected or confirmed to be compromised. The plan shall address what actions will need to be taken in the event of a compromise, to include impacts to any system software and hardware, existing cryptographic keys, and existing encrypted data.

Personnel assigned encryption key management responsibilities shall be trained in managing and maintaining control of cryptographic keys.

Management of encryption keys and key management software and hardware shall be conducted under the direct supervision of a County employee who has been through the Criminal Background Check as required by HR Procedural Memorandum #42.

County employees shall follow all cryptographic exportability laws and regulations restricting the international export of software containing encryption and barring or limiting the export of encryption technology.

3.4 Firewalls

In order to protect and manage access between the county's networks and the Internet, Firewalls and other access control devices are a critical component. Firewalls control access to internal and external IT resources. Access control devices, such as firewalls, which filter network traffic, shall segment the internal Fairfax County network infrastructure to support access policies developed by the designated owners of County information.

Fairfax County firewalls are the responsibility of DIT and shall be installed and configured following the Fairfax County Firewall Implementation Standards and Procedures. Agencies are not allowed to install independent departmental Firewalls. If a need is contemplated, then the agency must engage ISO for determination of appropriate measure, policy impact, authorization and implementation.

Interconnections of the Fairfax County network to the Internet or an extranet shall pass through firewalls that inspect transactions and validate access to County resources based upon source, destination, port, and protocol.

Firewalls shall be configured to deny all traffic by default and permit only those services approved by the ISO. Access to internal County information systems from any external network shall be limited only to services and protocols necessary for mission critical operations of Fairfax County information system resources. Ports and protocols that have inherent vulnerabilities and are unnecessary for business system functionality shall be denied implicitly at County firewalls. Requests for use of non-standard ports and protocols will be reviewed by ISO.

E-commerce servers including payment servers, database servers, and Web servers shall be protected by firewalls in a demilitarized zone (DMZ).

Firewall change requests shall be documented through established change management procedures and approved only when a clear business requirement or impact has been determined and a risk analysis has been performed by ISO.

Fairfax County firewalls shall be physically and logically protected to ensure only authorized personnel have access. Firewall administrators shall maintain and use individual accounts and passwords to authenticate to the firewall in accordance with access management and password policies.

Firewall configurations should be archived as part of configuration management and disaster recovery requirements.

Failover or high-availability features should be implemented for Fairfax County firewall systems when supported and acquirable. Logging shall be enabled on all firewall systems to ensure proper transaction history of network traffic across the enterprise for investigational purposes.

3.5 Identification, Authentication, and Access Control

3.5.1 Access Control

Data and system owners shall implement operational procedures and technical controls to ensure access to Fairfax County Government information and systems is based upon the principle of least privilege and an authorized need to know and access. The principle of least privilege, providing only the access necessary to perform assigned duties, shall be implemented to ensure the confidentiality, integrity, and availability of Fairfax County Government information systems and data.

Fairfax County information systems shall display a warning banner which identifies the system as a County-owned system, that access is limited only to authorized individuals for approved purposes, that all activity is subject to monitoring, and access indicates acknowledgment of these conditions.

County information systems shall initiate a session lock or timeout after a threshold of inactivity has been exceeded. Session locks shall remain enabled until the user again authenticates to the specific system or application.

Formal approval, usage restrictions, security standards, and deployment guidance shall be implemented prior to authorizing mobile devices to access County information or systems. Fairfax County Government shall monitor for unauthorized connections of mobile devices to County information systems and enforce protection and standard requirements for approved mobile device connections.

Fairfax County Government Information systems shall uniquely identify and authenticate general users, privileged or administrative users, processes, and systems.

Fairfax County Government public-facing resources (i.e. published via the Website) which may host privacy-related information systems shall uniquely identify and authenticate external users.

Authorization to create a user ID and password must be received from a designated approval authority. Requests for user, administrative, and system access must be approved according to formal access request procedures.

Remote access to Fairfax County information resources shall be capable only through approved and encrypted remote access implementations to ensure the confidentiality and integrity of remote access sessions. Fairfax County shall monitor for unauthorized remote access and violations of usage restrictions.

DIT may confine wireless communications to organization-controlled boundaries and monitor for unauthorized wireless connections. DIT shall scan for unauthorized wireless access points and take appropriate action if an unauthorized connection is discovered.

ISO shall disable internal wireless networking capabilities embedded within information systems or components when not intended for use in mission or business functions.

3.5.2 Account Administration

Provisioning of credentials (usernames/passwords) that grant access to County enterprise networks shall be maintained exclusively by the DIT.

Requests for County information system accounts shall maintain a formal and valid access authorization based on approved intended system usage within personnel mission and business functions.

Information system accounts shall be categorized based upon the access type and level of privilege required. Types of accounts may include user, system, application, guest, group, and temporary accounts.

Fairfax County information system accounts shall maintain group membership status based upon the access required to perform duties and must identify the user or process of the information system or privilege.

Users shall be assigned a unique account and user ID. Credentials shall not be shared or written down.

User access to Fairfax County systems shall be periodically reviewed and adjusted as necessary by the system owners to ensure that access is in accordance with the concept of least privilege. Agency Information Security Coordinators, Agency Access Control Administrators, or other designated personnel shall review and adjust access privileges when the role or responsibilities of a user changes or the user no longer needs access to County information systems or applications.

Accounts inactive for 60 days shall be disabled. Accounts for individuals on extended leave for more than 60 days shall be disabled unless specifically approved through the formal exception to policy process.

Fairfax County shall maintain a formal process to modify user accounts to accommodate events such as name changes, accounting changes, and permission changes.

Fairfax County information systems shall enforce account lockouts when a determined threshold of consecutive invalid login attempts by a user is exceeded. In this instance, accounts shall not be unlocked until released by an administrator.

Account management events, to include the creation, modification, and disablement of accounts, shall be audited and notifications sent to appropriate personnel. Fairfax County shall audit relevant account management events for abnormal time-of-day activity, duration, excessive privilege, and other atypical usage by information system accounts.

3.5.3 Identification and Authentication

Fairfax County information systems shall enforce complexity requirements for all user, administrative, and system account passwords. Complexity requirements shall ensure a minimum of 6 characters, to include uppercase letters, lowercase letters, numbers, and special characters when technically feasible for the system.

Passwords shall be treated as confidential information and be encrypted in storage and transmission.

Password minimum and maximum lifetime restrictions shall be enforced, and password reuse prohibited or minimized.

Access to all Fairfax County information systems, including but not limited to, databases, operating systems, applications, and file systems, shall require authentication with valid credentials.

User and System IDs, including administrator, system or service accounts, and network device IDs, shall have a private authenticator assigned.

Default passwords shall be constructed in accordance with this password policy and changed immediately upon first logon.

In the event the integrity of a password has been compromised, or suspected of compromise, the password shall be changed immediately, and ISO shall be notified.

Fairfax County information system users shall properly protect authentication credentials from unauthorized disclosure or modification.

County information systems shall obscure the display of passwords or other authentication information during the authentication process to ensure the confidentiality of the information from unauthorized use.

3.6 Passwords and Passphrases

Fairfax County information systems enforce complexity requirements for all user, administrative, and system account passwords. Users shall ensure to use a minimum of 6 characters when creating passwords, to include uppercase letters, lowercase letters, numbers, and special characters when technically feasible for the system.

Fairfax County information system users shall properly protect passwords from unauthorized disclosure or modification. Passwords shall not be shared with anyone internal or external to the County.

Users are required to maintain password secrecy. Passwords shall not be written down or stored in an unapproved retrieval system without proper security controls. Users shall not reveal their passwords in either electronic or verbal communications.

Passwords shall be changed immediately if the integrity of the password has been or is suspected to have been compromised and ISO shall be notified.

Passwords for all general user and administrative accounts shall be changed every 90 days and password reuse minimized according to system specifications. System and service accounts shall comply with the same requirements unless specifically approved through the formal exception process.

3.7 Screen Saver Usage

Screen savers are required to protect systems from unauthorized access and must be applied. DIT may force screen savers through system policy on Fairfax County information systems. User authentication shall be required to unlock the screen saver.

Screen saver timeout thresholds shall be enabled and set in accordance with the County standard image for workstations. Screen saver settings may not be modified without written authorization from ISO.

Screen saver images or desktop images will be removed if discovered to contain offensive or malicious content as defined in County policies regarding inappropriate content, or if determined to introduce unnecessary threats or vulnerabilities that could degrade the performance of the enterprise information infrastructure or system.

3.8 Security Breach Mitigation

Fairfax County agencies shall carefully assess the probability of unauthorized alteration, disclosure, or loss of information for which they are accountable and responsible. Agencies should perform security risk assessments for agencies business processes and operations.

Security assessments shall be performed only by approved DIT personnel, contractors, and vendors.

DIT shall use automated system tools that provide real-time notification of detected misuse, vulnerability exploitation, and unauthorized intrusion. Security baselines shall be developed, and tools will report deviations and exceptions to policy.

DIT shall deploy, maintain, and monitor security devices that will inspect Internet traffic and usage, email traffic and content, LAN traffic, protocols, and device inventory, and operating system security parameters and controls.

System and security event logs from various sources shall be collected and monitored for indications of misuse, intrusion, vulnerabilities, and misconfigurations. Log sources may include intrusion detection and prevention systems, firewalls, domain controllers, access control devices, vulnerability assessment utilities, file and member servers, applications, backup systems, printers, fax machines, workstations, mobile communication devices, and other County services and systems.

Authorized security personnel are authorized to perform security assessment or penetration tests against County systems and infrastructure with ISO and management approval to include password strength determinations, scanning for unauthorized and non-compliant devices and infrastructure, inappropriate sharing of devices, vulnerability determinations, and other assessment activities.

ISO personnel shall be granted physical and logical access to all facilities and systems required to respond to security issues and events, appropriately conduct assessments, perform and support investigations, and other security related functions.

Security violations, concerns, suspected and confirmed instances of successful or attempted intrusions shall be immediately reported to ISO, who will investigate.   System anomalies in system performance are normally indicative of system compromise and must be reported to the DIT IT Service Desk or ISO.

3.9 Infrastructure Protection

DIT shall be responsible for all aspects of the Fairfax County network infrastructure and will manage and administer all future developments, implementations, and enhancements to this infrastructure. Modifications, additions, and the removal of network management devices and configurations shall not be made without the approval of DIT and shall be governed by County Configuration and Change Management processes and procedures. DIT will establish operational and technical methods of protecting against unauthorized connections to the enterprise IT environment.

Fairfax County systems shall be designed, configured, and maintained according to County System Hardening Standards to adequately safeguard County information.   Baseline configurations and configuration deviations of Fairfax County information systems, network devices, and communications infrastructure will be documented, reviewed, updated, and available.

Network device addresses, services, and approved ports and protocols are allocated, registered, and managed centrally by DIT. Non-sanctioned or non-standard protocols shall be approved by DIT and the Information Security Office.

Fairfax County's internal network addresses shall remain private and protected using Network Address Translation. Systems requiring access to external networks shall have private addresses translated to a legal registered public address prior to transmission.

Interconnections of County network infrastructure with external third-party networks shall be approved by agency management, submitted through the County Change Management process, and coordinated with ISO. This includes connections to external telephone networks.

Routers, switches, hubs, taps, wireless access points, or any other network infrastructure devices shall not be installed on the Fairfax County network without approval from DIT and ISO. Network infrastructure or information systems that provide services shall not be extended or re-transmitted without DIT approval.

County information systems shall prevent access to system management functionality from general users through access control mechanisms.

County information systems shall protect against or limit the effects of Denial of Service (DoS) attacks by implementing technical controls and managing excess capacity, bandwidth, utilizing protection mechanisms against IP spoofing, implementing access filters, and establishing connection limits.

Fairfax County shall employ information systems to monitor and control communications at key system boundaries and connect to external networks or systems through managed interfaces in accordance with enterprise security architecture.

Internet traffic shall be routed through DMZs and associated technical equipment/solution which provide content inspection and analysis and allow for access policy management based upon County security policy and acceptable use requirements.

3.10 Intrusion Detection and Prevention Systems (IDPS)

Fairfax County shall utilize multiple types of IDPS technologies to achieve comprehensive and accurate detection and prevention of malicious events.

Fairfax County IDPS shall use operating system configurations that minimize the possibility of exploitation, unauthorized access, and system vulnerabilities. IDPS operating systems shall be current, patched, and configured according to industry best practices and County System Hardening Standards.

IDPS signature releases and software shall be kept current as to add new IDPS functionality, new detection capabilities, or refine existing detection capabilities.

IDPS administrators shall maintain and use individual accounts and passwords to authenticate to the devices in accordance with access management and password policies.

County IDPS shall be planned and deployed based on regulatory requirements and infrastructure of County networks and shall maximize the analysis of traffic transmitted and received.

Alert and notification functions for indications of intrusive activity from IDPS devices shall be enabled and monitored by information security personnel daily. Suspected and confirmed instances of intrusions shall be immediately reported to ISO.

3.11 Virus Detection

DIT shall implement and maintain a centralized anti-virus solution that provides automated protection for publicly accessible systems, perimeter devices, and internal server and client endpoints of the County enterprise infrastructure. Standalone and networked workstations and servers shall use the DIT-approved virus protection software and configurations.

Anti-virus software shall maintain centralized event logging for coordinated response and analysis.

Web and email gateway anti-virus software shall be installed and configured for real-time active monitoring at the perimeter according to DIT-approved configuration standards. Email file attachments shall be scanned in real-time to inspect for viruses or other malicious code.

Virus protection shall be installed on Fairfax County file servers and configured to identify and clean viruses that infect files shares.

Internet traffic shall be scanned in real-time to ensure that transmissions and downloads do not contain viruses or other malicious code.

Virus protection software on County information systems shall not be disabled, bypassed, or altered in any manner.

Virus pattern and scan engine updates shall be current and updated. New virus patterns and anti-virus engine updates shall be centrally acquired by DIT and distributed to County information systems after release by the anti-virus software vendor. The automatic update frequency of the virus protection software shall not be altered to reduce the frequency of updates.

Viruses which are automatically cleaned by the virus protection software shall constitute a security incident and be reported to ISO.

3.12 Wireless Communications

Wireless communications devices shall be subject to County regulations, rules, guidelines, and policies regarding the appropriate transmission and use of information and conduct. Wireless communications devices may include, but are not limited to, access points, laptop, tablets, PDAs, phones, digital assistants, pagers, wireless cards, and other information systems that can utilize wireless services or provide wireless capabilities.

Wireless access points and wireless communications devices shall be registered with a central wireless device database managed by DIT and shall be approved by DIT prior to deployment. Unauthorized devices shall be removed from service by DIT.

Wireless devices shall be DIT-approved vendor products and maintain approved security configurations.

DIT shall maintain a list of wireless standards to include approved wireless technologies, configuration standards, and best practice procedures for secure installations. Access points and wireless devices approved for County use shall be configured to meet the security controls standards established by DIT prior to deployment.

Wireless infrastructure design shall support a hardware address that can be registered and tracked for authorized use. For example, MAC-based authentication shall be employed by allowing only registered MAC addresses access to the access point.

Wireless systems shall support and employ strong user access control which authorizes the device or user against an external database approved by the Information Security Office. Users shall either be routed outside the Fairfax County firewalls or authenticate to a Fairfax County network segment based on the concept of least privilege once authenticated.

Information systems whether wired or wireless shall use an approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic when connected to wireless networks.

Wireless implementations shall maintain point-to-point hardware encryption of not less than 128-bit encryption. The transmission of County data wirelessly between clients, mobile devices, and other systems shall utilize DIT-approved encryption methods.

Wireless network default service set identifiers (SSIDs) shall be changed from their default vendor settings to unique names. SSIDs shall be non-trivial and difficult to guess and shall be a minimum of 10 characters in length.

Wireless LANs shall be segregated from traditional wired LANs using firewalls, VLANs, or DMZs.

Wireless access points are subject to periodic penetration testing and auditing by authorized personnel.

Access points shall be physically located in a secure and/or monitored area to prevent unauthorized access and physical tampering.

Access points shall be located appropriately within the intended broadcast area of service. Devices shall not be placed near windows or against the outside walls of buildings.

Access points shall be secured using an administrative password in accordance with the County Password Policy. Administrators shall ensure all vendor default usernames and passwords are removed from the device. Administration of the device through the wireless network is prohibited.

Fairfax County has the right to confine public wireless communications within its facilities and monitor for unauthorized use. Federal law enforcement authorities have the right to access and monitor use and content from public wireless access points.

ISO is authorized for wireless monitoring to include scanning for unauthorized wireless access points and initiating the appropriate incident response actions if an unauthorized connection is discovered.

Fairfax County agencies shall disable internal wireless networking capabilities embedded within information systems or components when not intended for mission or business functions.

4.0 Acceptable Use

4.1 General Principles

Fairfax County information systems are intended for performing County business.

Users of County information systems are expected to abide by this Acceptable Use Policy, as well as any other applicable local, state or federal laws and regulations, and County policies and procedures, regardless of whether a particular County information system is located internally or remotely, as in a cloud or similar type of off-site data storage, or whether data is transmitted, stored or received on mobile or fixed devices.

Examples of applicable information systems and resources may include, but is not limited to:

- Desktop PCs and Workstations
- Servers and network communications equipment
- Mobile devices such as laptops and tablets
- County issued cell phones, smartphones, and other voice and data devices
- County provided desktop telephones, projectors, and teleconferencing equipment
- Accessible enterprise resources such as email, instant messaging, internet, and other productivity software
- Remote access technologies that enable secure communications between County-owned and personal devices for instances of telework or other purposes
- Other enterprise technologies acquired and approved for enabling electronic access to County resources and data

4.2 County Ownership

Information systems and capabilities are provided to County users for the facilitation of County business. These systems and resources are explicitly owned by Fairfax County Government.

The County owns all property rights in any content or other matter created, received, transmitted, stored on, or deleted from, any County information system.

Any County information stored on a user’s personal mobile communications device or fixed device also is County property and may be viewed, accessed, retrieved, copied or disseminated by the County at any time.

4.3 User Privacy

Users of any County information system shall not have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by their use of these systems.

All user activity on any County information system and County-approved mobile communications or fixed devices is subject to monitoring, logging, auditing, review, dissemination and archiving by DIT. County agencies have the right to monitor any and all aspects of the County’s information systems, including any chat group, material downloaded or uploaded, and any email sent or received. This monitoring may occur at any time without notice and without the user’s awareness or permission. Internet traffic over County information systems shall be proxied and inspected for malicious code or inappropriate content prior to delivery to the user. Filters shall track user Internet activity, and be monitored for violations of this Acceptable Use Policy, as well as any other applicable laws, regulations, and County policies and procedures.

Storage of user personal information on County information systems is done at the user’s risk. Personal information stored on County information systems and mobile communication or fixed devices may be subject to mandatory disclosure under the Virginia Freedom of Information Act (VFOIA). Such information also may be subject to public disclosure or review by County officials. By using any County information system, the user agrees to surrender any data contained in such information system whether the data is owned by the County or alleged to be owned by anyone other than the County. Personally-owned mobile devices that have been formally approved for access to County systems or data may also need to be provided to DIT in the instance that a VFOIA request is made to the County, a County employee, or County agent, for DIT to make a determination if any County data on the personal device is relevant to the request.

Personally-owned mobile communication devices which have been approved for access to County information or technology resources may be subject to confiscation by DIT, and/or may be released to law enforcement, in the event of an information-system or data security breach, or other investigation.

4.4 Confidential Information

Users shall comply with all laws, regulations, and County policies and procedures prohibiting or limiting the disclosure of confidential information, including but not limited to County client personal information (e.g. medical records, financial information, and social security numbers) tax information (e.g. information of any person firm or business with respect to any transactions, real and personal property, income or business of the taxpayer) and County employee personal information (e.g., medical records, financial information, and social security numbers). Confidential information transmitted on County information systems shall be sent only to those recipients who are authorized to receive such confidential information.

Users shall take all steps necessary to protect the privacy of confidential information maintained by the County from unauthorized access. These measures include, but are not limited to, enabling password protection on any fixed or mobile system, or otherwise locking and closing computer screens when leaving even for brief period, and logging off or terminating a system session when access is no longer needed or the user is leaving for the day.

Users shall follow all Federal, Commonwealth, and County policies and guidelines defining data classification and protection requirements. These requirements include, but are not limited to, the following:

- Information classified as Confidential or Sensitive shall only be stored on approved storage devices that use encryption.
- Users shall not use non-County information systems or devices to send, forward, receive or store information classified as Confidential, Sensitive, or for Internal Use, unless approved by DIT in writing.
- Users shall not use non-County messaging utilities such as Hotmail, Yahoo Mail, AOL Mail, and Google Mail to send, forward, or receive information classified as Confidential, Sensitive or for Internal Use.
- Information classified as Sensitive being sent outside of any County information system shall be specifically labeled as such and shall have restricted distribution only to those recipients who are authorized to receive such Sensitive information.
- Information classified as Confidential or Sensitive transmitted to external networks shall be encrypted in accordance with DIT encryption standards.

4.5 Incidental Personal Use

Personal use of any County information system is use that is not related to the purpose for which the County has granted the user authorized access. In general, incidental personal use of the County's information systems, such as Internet access and email, is permitted, unless the agency in which the user works restricts all incidental personal use of information systems.

Personal use of information systems is prohibited when it:

- Interferes with the user's productivity or work performance, or with the productivity or work performance of other users;
- Adversely affects the efficient operation of the information system or the County; or
- Is illegal, or violates this Acceptable Use Policy, the County's Standards of Conduct, the County Executive's Information Technology Security Policy Memorandum Number 70-05, or any other County policy or procedure.

Users must present their personal communications using County information systems in such a way as to make clear that these communications are personal, and not communications from their agency or the County or from the user in his or her capacity as a representative of the County.

Storage of personal email messages, voice messages, files, and documents on County information systems shall be kept to a minimum. Any such storage which DIT determines interferes with the efficient operation of the County's information systems is subject to removal by DIT without the notice or consent of the user.

4.6 Prohibited Use

Certain activities are prohibited when using County information systems, applications, data and resources, whether on County –owned or personally–owned devices, except when County management has determined such activities are necessary for the performance of a user's official duties. These prohibited activities include, but are not limited to, the following:

- Accessing, downloading, transmitting, printing, or storing information with sexually explicit content.
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, violent, harassing, or discriminatory messages or images.
- Accessing or downloading gambling sites.
- Pursuing personal profit or gain or engaging in outside employment or personal business, unauthorized fundraising or political activities.
- Engaging in any prohibited activity described in the County Executive's Information Technology Security Policy Memorandum Number 70-05, or any other County policy, regulation or guidance related to the use of County information systems.
- Unauthorized downloading, printing, or transmitting of information protected by federal or state copyright laws.
- Misusing or misapplying County information system privileges.
- Using software in violation of County vendor licensing agreements.

4.7 Information System Security

Users shall respect the confidentiality and integrity of any County information system, be familiar with County information-system security policies and procedures and report any security weaknesses or breaches in County information systems to DIT.

Users shall respect security controls for County information systems and not attempt to or circumvent those controls.

Users shall not access or attempt to access any County information system without authorization from DIT to do so.

Users shall refrain from activities that intentionally or inadvertently disrupt, impair, or undermine the performance of County information systems. These activities include, but are not limited to, the following:

- Intentionally causing physical or logical damage to a County owned information system or resource
- Downloading computer viruses or malware or otherwise introducing malicious code into a County information system
- Using Internet-based proxy servers or anonymizers, or any other tool, device or action that makes Internet activity untraceable, to bypass Web-filtering security mechanisms established on County information systems;
- Downloading, installing, or running security programs or utilities that reveal weaknesses in the security of a County information system, including but not limited to password cracking programs, network reconnaissance and discovery applications, key loggers, packet sniffers, network mapping tools, and port scanners, without prior approval from DIT in writing; or
- Consuming excessive bandwidth through actions including but not limited to placing a program in an endless loop, printing excessive amounts of paper, and sending chain letters and unsolicited mass emails.

Files and other content downloaded from the Internet, including but not limited to non-standard shareware, free software, peer-to-peer software, and information-sharing software, is subject to prior approval from DIT in writing. This approval may be conditioned upon DIT checking the downloaded files or content for viruses, trojans, malware, or other potentially malicious content.

Users shall refrain from divulging to unauthorized persons any details regarding County information systems or architecture unless previously authorized.

The use of passwords to access County information systems and County-approved mobile communications devices is for the protection of the County, and not any user. Users shall take reasonable steps to prevent the disclosure of their usernames, passwords, security tokens, or other similar information to unauthorized users.

Users shall not use cloud or Internet-based hosting services to store or share County data unless specifically approved by DIT in writing and acquired through terms that include the requirement for compliance with DIT security standards in a contract approved by DPSM.

Users shall take all steps necessary to complete logoff or other termination procedures when finished using any County information system. At a minimum, users should take such steps to logoff of terminate from a County Information system at the end or every workday.

Users of County-approved mobile communications devices shall ensure that precautions are taken to prevent theft or loss. Unattended County mobile communications devices shall be physically secured (e.g., locked in an office, desk drawer or filing cabinet; attached to a desk or cabinet by a cable lock system) when unattended. Any user must immediately report to DIT any loss or theft of any mobile communications device containing any information from a County information system.

Users shall not connect personally-owned, or other non-County owned, equipment or devices, including, but not limited to, USB or other storage or memory devices, iPads or iPods, PDAs, tablets, BlackBerry devices, mobile phones or cameras, to the County network infrastructure in any manner without proper approval. These devices should not be connected to County systems for purposes of charging power, transferring personal audio, video, or images as non-County owned electronic devices may introduce unnecessary risk to County systems and data.

Remote access to County information systems using a personally owned fixed device or mobile communications device shall only be permissible through DIT provided and supported remote access software applications, protocols, delivery mechanisms, and if necessary, DIT provided and supported anti-virus software.

Users with remote access shall ensure that their personally-owned fixed device or mobile communication device remotely connected to a County information system is only connected to legitimately secure networks, such as a personally-owned home network under complete control of the user, or a validated provider network, and that their fixed device or mobile communications device maintains basic security controls (e.g., password protection) to prevent unauthorized access to all County information systems.

The method of storing information on a personally owned fixed device or mobile communications device shall comply with DIT information-system security requirements.

Users shall immediately report the loss of any personally owned fixed device or mobile communications device used to access County information systems to DIT. In the event of a lost or stolen device, the County reserves the right to clear its data from the device by any available technical means.

4.7.1 Electronic Messaging Systems

County users are responsible for the content of all text, audio-video or images stored, transmitted, or received over the County's electronic messaging (i.e., email) and other collaboration systems, such as instant messaging.

All messages communicated on County email systems shall contain the sender's name. Email or other electronic communications shall not be sent on County email systems which mask or attempt to mask the identity of the sender.

Users shall make reasonable efforts to validate the authenticity of emails received prior to opening any attachments or clicking on links.

The following activities are among those that are acceptable uses of County email systems:

- Communicating and exchanging information directly related to the mission, charter, or work tasks of the County.

- Communicating and exchanging information for professional development, to maintain currency of training or education, or to discuss issues related to the County business.

- Applying for or administering grants or contracts for County research or programs.

- Conducting advisory, standards, research, analysis, and professional society activities related to the County business.

- Announcing new laws, procedures, policies, rules, services, programs, information, or activities.

- Incidental personal use, in accordance with Section 4.5.

Users of County email systems shall not give the impression in their communications to persons receiving such emails that they are representing, giving opinions, or otherwise making statements on behalf of the County or any agency of the County, unless otherwise authorized to do so. Where appropriate, a disclaimer shall be included, unless it is clear from the context that the email's author or sender is not representing the County. An example of a disclaimer is: "The opinions expressed are my own, and not those of Fairfax County."

4.7.2 Internet and Intranet

Fairfax County WEB sites which includes the external facing public WEB sites and content, and, the County-wide Intranet site for internal county applications and services access (FairfaxNet) and other collaboration tools, are for County business purposes. The County provides general access to the Internet from County networks and devices to include Social Media. Also, when an employee is issued a county mobile device, access to the Internet from that device is identified as a County device. By accessing the Internet from any County IT resource, county users are identified as connecting from Fairfax County. Content and use of all County Internet and Intranet sites shall comply with County IT Security policy and standards, County HR policy and Standards of Conduct, and acceptable use policies as well as guidelines included in the Public Website Content Policy, FairfaxNet Policy (Intranet/collaboration portal), any other applicable County policy to include agency specific compliant procedure, standard, or guideline. This includes use and actions on an external website from Fairfax County networks and devices.

Web filtering technologies are implemented that governs policy and access to the Internet from Fairfax County network(s) and devices to protect the County's technology systems and data from exposures to malicious code, excessive bandwidth uses, and also to block content and internet sites deemed to present in its use significant risk, inappropriate or illegal. County users shall not try to circumvent the implemented WEB filters or otherwise tunnel through authorized sites to gain access to unauthorized sites. Internet sites which are blocked but are later determined to be necessary to conduct business on behalf of Fairfax County can be submitted to infosec@fairfaxcounty.gov for review and consideration.

Users shall not download or paste any application, service or inappropriate data from the Internet site to County Internet or Intranet sites without authorization by DIT.

Users shall not use the Internet to purchase, obtain, or offer products or information for County purchases outside of County Purchasing rules and procedures or without prior approval from DPSM.

4.7.3 County Social Media

The County uses specific social media platforms to deliver public information, communications engagement, perform customer service, and conduct transactions, and communicate official business with constituents, stakeholders, partners, the media and the public in general. Agencies may establish an official Fairfax County Social Media presence which requires an authorized user/administrator and/or moderator. The County also allows employees general access to Social Media.

The IT Security Policy requirements apply to the use of Social Media platforms and capabilities. Informational content and services distributed and published through the County's official social media outlets shall be governed by the IT Security Policy, the Office of Public Affairs Social Media Policy and Guidelines, and any other applicable County policy, procedure, standard, or guideline.

Access to non-County approved social media platforms, and diversion in implementation and use of authorized Social Media can be granted through the executive exceptions process that includes DCEX, Office of Public Affairs, DIT and ISO.

4.7.4 Personal Social Media

This Policy shall not seek to regulate users establishing and using personal social media accounts and other similar communications (e.g., personal Internet sites; blogs) for personal purposes outside of the workplace and using non-County equipment, resources, and information systems.

Personal social media use, as well as the use of other similar communications tools hosted externally or internally on County hosted resources such as, but not limited to, forums and blogs, shall include no statements or depictions stating or implying that the user represents the County, is making an official statement of County policy, or is making a statement or depiction with the County's permission, whether implied or expressed, unless the user has received documented permission from the appropriate County authorities to communicate on the County's behalf in the non-County venues.

Users are encouraged to include in personal electronic communications discussing or relating to County business a disclaimer along the following lines: "The views I express are my own and do not reflect the official view or position of Fairfax County."   In accessing personal social media from the County IT environment, users should follow the County standards of content. Users may not download or copy content from their personal social media accounts to Fairfax County systems without permission.

4.7.5 County Mobile Communication Devices

Mobile communication devices approved by DIT to access County information systems shall only use County-approved remote access applications or methods and shall be compliant with established DIT technical standards and policies.

Upon separation from the County, or for any other reason deemed necessary by DIT to protect the County, any user's access to any County information system and all County mobile communications devices shall be terminated, and the user shall return to DIT all County-owned mobile communications devices issued to him or her.

4.7.6 Personal Mobile Communications Devices

Any personally owned mobile communication devices shall not be connected to County information systems, nor be used to store County information, unless approved by DIT in writing, and only when that use is consistent with the remote access technologies provided and intended by DIT. A user must sign a Mobile Device Agreement to be authorized to use his or her personally owned mobile communications device(s) to access any County information system.

Access privileges to County information systems through a personally owned mobile communications device shall be terminated upon the user's separation from the County or for any other reason deem necessary by DIT to protect the County.

4.7.7 Remote Access

Remote access to County information systems shall only be permissible through DIT-provided and supported remote access software or services.

Remote access shall be provided after a determination has been made that access is required to perform assigned duties, or the user is defined as "essential" personnel by the County. Remote access shall be requested using the Mobile Workforce IT Tools form.

4.8 Violations

Engaging in prohibited uses of the County's information systems shall be considered a violation of this Acceptable Use Policy and the County's Standards of Conduct, and may subject the violator to discipline, up to and including dismissal.

The County reserves the right to deny further access to its information systems when it believes such action is necessary to protect system security and performance. Denial of access may include, but not be limited to, revocation of accounts, passwords, software, and hardware.

Anyone who suspects a user of any inappropriate use of County information systems should take the following actions:

- Direct questions concerning any inappropriate use to their supervisor, DHR's Employee Relations Division, and/or DIT.
- Complete and submit the "Incident Reporting Form"

When responding to a possible violation of the law or County policy involving the use of County information systems, DHR and DIT may involve staff from other County agencies, including but not limited to Internal Audit, the Office of the County Attorney, and the Police Department.

REFERENCES

Federal Copyrights Act, Pub. L. No. 94-553 (1976)
Federal Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474 (1986)
Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996), (“HIPAA”)
Virginia Freedom of Information Act, Va. Code §§ 2.2-3700 through 2.2-3718
Virginia Government Data Collection and Dissemination Practices Act, Va. Code §§ 2.2-3800 through 2.2-3809
Virginia Computer Crimes Act, Va. Code §§ 18.2-152.1 through 18.2-152.14
Virginia Public Records Act, Va. Code §§ 42.1-76 through 42.1-91
Virginia Records Management Retention and Disposition Schedules
Fairfax County Fraud Policy (PM 02-04)
Fairfax County Employee Handbook
Fairfax County Standards of Conduct
Fairfax County Telework Program
Fairfax County HIPAA Compliance Policy (PM 02-09)
Fairfax County Public Website Content Policy (PM 13-04)
Fairfax County Governance and Management of County IT Staff and Assets (PM 70-07)
FairfaxNet Policy
Office of Public Affairs Social Media Policy and Guidelines
Fairfax County Employee Clearance Record (PM 11-33)
DIT Change Management Policy #9
Second Edition Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology (NIST), SP 800-21-1
Recommended Security Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology (NIST), SP800-53
An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, National Institute of Standards and Technology (NIST), SP800-66
Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, PCI Security Standards Council
Creating a Vulnerability and Patch Management Program, NIST SP800-40

DEFINITIONS

Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Agency Access Control Administrator (AACA): Responsible for managing agency user access control privileges and monitoring agency access control and audit logs.

Agency Head: The Agency Head is ultimately responsible for carrying out the security policy and for the development and implementation of the agency information technology security function within their agency. The Agency Head has the ultimate responsibility to ensure that all agency information systems, regardless of medium, are used, maintained, disclosed, and disposed of according to law, regulation, policy, and standards. The Agency Head shall appoint an AISC within their area of responsibility to develop, implement, and maintain the Information Security program within their agency.

Agency Information Security Coordinator (AISC): Responsible to the CCSPO for administering the information security functions within their agency. The AISC is the internal and external point of contact for all information security matters at an agency.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a disruption.

Business Continuity Plan: A plan which allows critical business functions to continue in the event that primary business facilities or resources are not available.

Business Impact Analysis: An analysis which identifies information, applications, processes, and systems required to support critical business processes and functions.

Change: Any implementation of new functionality, interruption of service, repair of existing functionality, or removal of existing functionality.

Change Management: The process of controlling modifications to hardware, software, firmware and documentation to ensure that information systems are protected against improper modification before, during and after system implementation.

Chief Technology Officer (CTO): The Deputy County Executive holds the position of Chief Technology Officer (CTO) and holds the authority and accountability to implement security policies, standards, and guidelines to protect County information and systems. The CTO shall coordinate a County-wide program to identify and resolve security problems, review roles in matters impacting security and provide support to management and data owners in the performance of their security responsibilities. The CTO has delegated authority to the Director of the CCSPOO to maintain and staff a centralized security function to implement and control the County Information Technology Security Program. The CTO has appointed a Fairfax County Chief Cyber Security and Privacy Officer (CCSPO) to lead this function.

Chief Cyber Security and Privacy Officer (CCSPO): Responsible to the CTO for administering the information security program within the County. The CCSPO is the County's internal and external point of contact for all information security matters. The designation of the Chief Cyber Security and Privacy Officer is intended to establish clear accountability for development and maintenance of policy for information systems security management activities, provide for coordination and review of the County's information security program, and ensure greater visibility of such activities within and between County agencies.

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization.

Commercial off the Shelf (COTS): Software that is commercially available from a vendor.

Custodian: Guardian or caretaker; the holder of data, the agency or department charged with implementing the controls specified by the owner.

Department of Information Technology (DIT): The agency responsible for information systems, networking, and data management.

Disaster Recovery Plan: The preplanned sequence of events that allows for the recovery of an information system facility and information systems and applications.

Electronic Mail (email): Any message, image, form, attachment, data, or other communication sent, received or stored within an electronic mail system.

Electronic Mail System: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Firewall: A rule-based hardware or software control device that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Host: A computer system that provides computer service for a number of users.

Identity Management (IDM): The task of controlling information about users on computers. Such information includes information that authenticates the identity of a user, and information that describes information and actions they are authorized to access and/or perform. It also includes the management of information about the user and how and by whom that information can be accessed and modified.

Information: Any and all data, regardless of form, that is created, contained in, or processed by, information systems facilities, communications networks or storage media.

Information Attack: An attempt to bypass the physical or information security measures and controls protecting a system. The attack may alter, release or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information systems (IS): Any and all computer-related equipment and components involving devices capable of managing, transmitting, receiving or storing information or data including, but not limited to, a USB drive, CD-R, laptop or personal computer, personal digital assistant (PDA), cell phone, handheld computer, servers and computer printouts. Additionally, it is the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit information.

Information Security Office: Responsible for the maintenance, installation, operation, and periodic review of centralized security controls. This office will also monitor implementation and compliance with County-wide policy and security directives and provide status reports to the CTO.

Internal Auditor: Ensures that an agency's information systems are being adequately secured, based on risk management, as directed by the CCSPO acting on delegated authority for risk management decisions.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and educational institutions.

Internet of Things: The "Internet of Things" (IoT) refers to technology implementations in which network and computing capability is extended to non-traditional devices, rather than non-traditional computing devices such as computers, smartphones and tablets, allowing these devices to create, transmit and receive data through the internet. Examples of devices that may fall into the scope of "Internet of Things" include security systems, environmental monitoring sensors, vehicles, electronic appliances, vending machines and more.

Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's Intranet is usually protected from external access by a firewall.

Local Area Network (LAN): A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Off-site Storage: Based on data criticality, off-site storage should be in a geographically different location from the Fairfax County campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on the Fairfax County campus may be appropriate.

Owner: The manager or agent responsible for the function, which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

Portable Computing Device: Any easily portable device that can receive and/or transmit data to and from Information systems. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers and cell phones.

Production System: A computer system used to process an organization's daily work. Contrast with a system used only for development and testing or for ad hoc inquiries and analysis.

Program Manager: Assigned information systems ownership; responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures.

Risk Assessment: The process of evaluating threats and vulnerabilities, both known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system.

Security Incident: A successful or unsuccessful unauthorized entry or information system attack. Security incidents may include unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. Ay incident may also include any violation of security policy or acceptable use agreements.

Server: A server is a system that provides services to client systems. The computer that a server program runs in is also frequently referred to as a server (though it may contain several servers and client programs).

Service Set Identifier (SSID): The public name of a wireless network. All wireless devices on a Wireless Local Area Network (WLAN) shall employ the same SSID in order to communicate with each other. SSIDs are also referred to as a network name because essentially it is a name that identifies a wireless network.

Spam: Mass-delivered, unrequested advertising delivered via email.

Strong Passwords: A password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, Social Security number, etc.

System Administrator: Person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Systems Development Life Cycle Standards (SDLCS): A set of procedures to guide the development of production application software and data items. The SDLCS includes design, development, maintenance, quality assurance and acceptance testing.

Technical Manager: Assigned custodian of information systems; provides technical facilities and support services to owners and users of information. The technical manager assists program management in the selection of cost-effective controls to be used to protect information systems and is charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

Trojan: Destructive programs that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by email or on a removable media device, often from another unknowing victim, or may be urged to download a file from a Website.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerabilities.

User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

Vendor: Someone who exchanges goods or services for money.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive results. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in programs that allow users to generate macros.

Web Log (Blog): A public website where users post informal journals of their thoughts, comments, and philosophies, updated frequently and normally reflecting the views of the blog's creator.

Web Page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

Web Server: Information systems that host and deliver Internet services.

Website: A location on the World Wide Web, accessed by typing its address (Universal Resource Locator, or URL) into a Web browser. A Website always includes a home page and may contain additional documents or pages.

Wiki: A type of website that allows the visitors to easily add, remove, and otherwise edit and change content, sometimes without the need for registration. The term Wiki also can refer to the collaborative software itself (Wiki engine) that facilitates the operation of such a Website.

World Wide Web (WWW): A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Microsoft Internet Explorer.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is like a virus in that it makes copies of itself, but different in that it need not attach to files or sectors at all.

INDEX

ATTACHMENT A: EMPLOYEE TECHNOLOGY USE AGREEMENT

DEPARTMENT OF INFORMATION TECHNOLOGY

CONCERNING ACCESS TO, THE SUPPORT OF AND USE OF INFORMATION SYSTEMS AND COMMUNICATIONS TECHNOLOGY At FAIRFAX COUNTY, VIRGINIA

I, ____ working as an employee in the Department of Information Technology (DIT), recognize my legal and ethical obligation to conduct my work on any Fairfax County information or communications system using computer hardware and/or software (programming languages, operating systems, databases, third party application software and databases (COTS, WEB based, and 'Clouds'), system utilities, security solutions, data or voice communications software and electronics, devices (county issued or when using personal device attached to the county network conducting county IT work), and the *Internet including Social Media*), herein referred to as 'technology', in a responsible and accountable manner. My purpose in using computer and Internet based technology is to perform technology related work for Fairfax County Government and any others in conducting County business in the Department of Information Technology (DIT) in support of Fairfax County Government agencies and business functions, and therefore I am subject to the technology standards, IT Security and Privacy policies, procedures, and ethics and behavior policies of Fairfax County Government, and any public law that governs use of technology. As a condition for and in consideration of being given access to the information technology systems, equipment, and data, I agree that:

I will not use Fairfax County technology systems to access any information available or acquired from County technology systems for any reason except for purposes directly related to my job assignments and responsibilities as defined by DIT and the agencies I support as required. I will not use Fairfax County technology systems or databases to disclose any information available or acquired from the computer systems or County databases for any reason except for purposes directly related to my job assignments and responsibilities as defined by DIT and Policy. I understand that any work I perform for Fairfax County that develops systems, logic, or data is the property of Fairfax County, and I cannot take or send such products without express permission of appropriate Fairfax County authority. I understand that taking or moving data or information trusted for use by me in my job assignments to unauthorized venues outside county systems to include personal e-mail stores, personal hard media, external database unless authorized, or personal Internet/Social Media account is prohibited. Further, misuse of any data in any format covered under any Federal, State, or local laws, e.g. sensitive data is strictly prohibited.

I understand that a user agency may ask me to sign a separate agreement relating to the privacy and security of the information that the user agency owns and administers.

I will use vendor provided software and/or utilities only in accordance with such provisions as may have been agreed to between the vendor/licensor and Fairfax County. I will not deliberately violate any copyright laws or agreements as stated or implied in my use of the software. I recognize that to do so makes me personally liable for applicable penalties.

I further understand that the deliberate misuse of Fairfax County software, technology systems or assets which results in the change, damage or destruction of County systems, programs, and/or data is considered destruction of County property and may result in disciplinary action taken against me. Such may also result in disciplinary action may include dismissal or possible prosecution for my destruction of County property. Violation of IT/Cyber Security Policy which is 'no tolerance' may also result in formal disciplinary action. I further understand and recognize that there are criminal penalties for deliberate destruction of government property, misusing government information and for the improper use of government information.

I have completely read and fully understand the terms of this agreement and accepted these terms.

____ _______________
DIT Employee Signature Date

I accept this agreement on behalf of Fairfax County, Virginia.

____ _______________
DIT/Division/Program Manager/Supervisor Signature Date

____ _______________
ISO Date

ATTACHMENT B: CONSULTANT/CONTRACTOR

Fairfax County DEPARTMENT OF INFORMATION TECHNOLOGY

IT Services Provider CONSULTANT/CONTRACTOR AGREEMENT

CONCERNING ACCESS TO AND USE OF INFORMATION SYSTEMS and COMMUNICATIONS TECHNOLOGY AT FAIRFAX COUNTY, VIRGINIA

I / this firm____ working as a consultant/contractor/services provider for Fairfax County Government with access to county technology and communications systems, recognize my/our firm's legal and ethical obligation to conduct work on any Fairfax County information or communications system using computer hardware and devices, and/or software (programming languages, operating systems, databases, third party applications software (COTS) and Web based or 'cloud' applications), system utilities, security solutions, monitoring systems, and, data or voice communications software and electronics, Internet capabilities, etc. and county data/content herein referred to as 'technology', in a responsible manner and within the guidelines of the County's IT Security Policy and/or firm's contract. My/our purpose in using computer based technology is to perform work for Fairfax County which includes accessing Fairfax County systems through the Internet, and therefore we are subject to the standards, IT Security and Privacy policies, and ethics and behavior policies of Fairfax County Government. As a condition for and in consideration of being given access to computer systems, data, the network, internet, and, Fairfax County computer center(s), IT galleries, server rooms, network core facilities, third party hosting centers and 'clouds' where county services are provided or supported, I/we affirm that:

I/our firm possess the professional credentials that I or my firm has represented in being hired to perform my/our duty and assignments, and that I/our firm representatives have successfully passed a certifiable criminal background check.

I/our firm will not use Fairfax County technology systems or our firm's systems to access any information available or acquired from the technology systems for any reason except for purposes directly related to our (firm's) job assignments and responsibilities as defined by my/my firm's contract and assignment with the County. I/we will not use Fairfax County technology systems to disclose any information available or acquired from Fairfax County systems for any reason except for purposes directly related to my/my firm's contract and job assignments and responsibilities for such use as defined by DIT and contract(s). I/we understand that any work I/we perform for Fairfax County that develops systems, logic, or data is the property of Fairfax County, and I/we cannot take or send such products or data without express permission of appropriate Fairfax County authority. I/we will exercise due diligence in providing policy and oversight of our firm's contractors and subcontractors. I/we understand that a user agency may ask me/ my firm to sign a separate agreement relating to the privacy and security of the information that a user agency administers, such as for HIPAA, PCI, PII, and/or other Data Privacy Cyber Security laws.

I/ our firm will use vendor provided software and/or utilities only in accordance with that vendor's license, and such provisions as may have been agreed to between such vendor and Fairfax County. I/we will not deliberately violate any copyright laws or agreements states or implied in my/our use of the software. I/we recognize that to do so makes me/my company liable for any applicable penalties and may lead to my/our firm's immediate dismissal from the County's engagement.

I/our firm further understands that the deliberate misuse of Fairfax County technology, data, and/or software which results in the change, damage or destruction of County systems, programs, and/or data is considered destruction of County property and may be considered a breach of contract and/or a criminal offense. I/we understand that our firm may be liable to include immediate release from the engagement for breach of the Fairfax County IT Security Policy, and possible prosecution for the actions of my/this firms actions in the destruction of County property, misuse or theft of classified (sensitive) data. I/we further understand and recognize that there are criminal penalties for deliberate misuse of government information.

I/we have completely read and fully understand the terms of this agreement and accept these terms.

____ Name of Firm

____ __________________

Firm's Consultant/Representative Signature Date

____ __________________ Firm

Authorized Representative Signature Date

I acknowledge receipt of this agreement on behalf of Fairfax County, Virginia.

____ __________________ Firm

County IT Security Officer Date

ATTACHMENT C: REQUEST FOR WAIVER/EXCEPTION

Department of Information Technology Information Security Office
Procedural Memorandum 70-05 Revised

Procedural memorandum 70-05 Revised provides for the availability (continuity), integrity, and, confidentiality and privacy of its applicable information resources. The Information Security program is designed to address the protection of information assets regardless of electronics or digital format (e.g. voice, tape, disc, etc.), or, processing method or platform (e.g.
mainframe, server, personal computer, PDA, e-mail, Internet, etc.), and the integrity of use of the information assets. The policy applies to all County agencies and facilities that use County information technology, vendors and contractors that provide information products and services to the County, and to individuals and organizations external to the County government that exchange data and information with the County.

Please complete this form for all requests for exemptions from PM 70-05 Revised. This form must be signed by the requesting **Agency Director** and submitted to the **Chief Information Security Officer (CISO)** for review. Final determination will be made by the **Deputy County Executive for Information and Compliance** or **CTO**. The CISO will make notification of waiver. Agency activities that are approved for waiver exemptions accept responsibility for incidents that result in system problems, investigations or audits, or, interventions requiring CISO or DIT support and agree to pay for costs that may be incurred as a result. **The IT Employee Agreement on the reverse of this form must be signed by each employee granted permissions under this Waiver.**

By signing this request, I understand that compliance with Fairfax County Information Technology Security policies and standards is expected for all organizational units, information system, and communication systems. I have read the abovenamed policy or standard, and I believe that the control(s) described therein should not be required of the following organizational units, information system, or communication system (described below).

I understand that a control deficiency in one network-connected system can jeopardize other information systems because erroneous data may be inherited, or because a conduit for an intruder to enter Fairfax County systems may be created.

I understand that an exception to information security policies and standard is appropriate only when it would: (a) adversely affect the accomplishment of Fairfax County Government business or fulfilling the mission of my agency, and/ or (b) cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance.

I have an assessment of the risks associated with being out-of-compliance with the above-mentioned policy or standard. Risks which have been assessed have been presented to and/or reviewed with the CISO, the CTO and, if appropriate, the Senior IT Steering Committee.

Name of Requestor: ____ **Date:** ______________________

Agency: ___________________________________ **Sub Agency/Office/Division**: ______________________

Location(s): ____

Please describe your request below, **identify the section(s) of PM 70-05 Revised for the request for exemption, and provide a business justification for each exemption in an attachment. All exemptions must be identified.**

I accept responsibility for this decision to be out of compliance with Fairfax County Government information security policies and/or standards. I also understand that this exception must be renewed annually.

Agency Director's Name: ______________________ Signature: __________________________ Date: _____________

DIT USE ONLY

❏ Approved Platform Technologies Div., Director Signature ____________________________________ Date: __________

❏ Denied CISO Signature: ____ Date: ________________________

Remarks: ____

____

IT Exception to Policy v. 8 2013 Page 1 of 2 (reverse side)

Employee Agreement
Concerning the Support and Use of Information Systems and Communications Technology at
Fairfax County, Virginia

I, _______________________________, working as an employee, consultant, volunteer or partner, with Fairfax County Government, have been granted an exception to IT Security Policy enabling permissions or access to IT systems or resources beyond the regular access provided to regular County users. I recognize my legal and ethical obligation to conduct my work on any Fairfax county information or communications system using computer hardware and/or software (programming languages, operating systems, databases, third party application software and databases (COTS), system utilities, security solutions, data or voice communications software and electronics), and the Internet and Web-based applications including WEB 2.0 and Social Media sites herein referred to as "technology", in a responsible and accountable manner in performance of my approved County duties, and will not abuse these privileges. I understand that my use of information technology is to perform work for Fairfax County Government business functions, and therefore I am subject to the county's technology standards, IT Security and Privacy policies, procedures, and ethics and behavior policies of Fairfax County Government, and any public law that governs use of technology.

As a condition for and in consideration of being given access to the information technology systems, equipment, and data, I agree that:

I will not use Fairfax County technology systems to access any information available or acquired from the technology systems for any reason except for purposes related to my job assignments and responsibilities as defined by management for my assignments as required. I will not use Fairfax County technology systems to disclose any information available or acquired from the computer systems for any reason except for purposes directly related to my job assignments and responsibilities as defined by County IT and departmental policy. I understand that my agency may ask me to sign a separate agreement relating to the privacy and security of the information that my agency owns and administers. I also understand that I maintain no expectation of privacy in my use of Fairfax County Government information systems and that my activity may be monitored as deemed necessary to protection County information and systems.

I will use vendor provided software and/or utilities only in accordance with such provisions as may have been agreed to between the vendor/licensor and Fairfax County. I also recognize that when using Internet-based sites, I am not granted authorization to enter into contractual agreements on behalf of Fairfax County Government without authority and understand that all internet activity originating from Fairfax County government systems is traceable. I will not deliberately violate any copyright laws or agreements as stated or implied in my use of technology. I recognize that to do so makes me personally liable for applicable penalties.

I further understand that the deliberate misuse of Fairfax County software, technology systems or assets which results in the change, damage or destruction of County systems, programs, and/or data is considered destruction of County property and may result in disciplinary action taken against me. Such disciplinary action may include dismissal or possible prosecution for destruction of County property. I further understand and recognize that there are criminal penalties for deliberate destruction of government property, misusing government information and for the improper use of government information.

I have completely read and fully understand the terms of this agreement and accept these terms.

______________________________	____________________
Employee Signature	Date

(If not applicable, please initial here ____________.)

ATTACHMENT D: PCI-DSS COMPLIANCE AND COUNTY SHARED RESPONSIBILITIES

SUMMARY

The Payment Card Industry Data Security Standard (PCI-DSS) was developed to enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI-DSS provides a baseline of technical and operational requirements designed to protect credit card account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI-DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Guidance on Fairfax County's Payment Card Acceptance Program can be found in Financial Policy Statement 241: Payment Card Acceptance Program.

Technical and operational requirements to ensure the security of County credit card payment processing environments are defined in the PCI-DSS. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

The following document is intended to define a high-level overview of the shared responsibilities between the Agency, Department of Information Technology, and Department of Finance in implementing the requirements of the PCI-DSS to achieve and maintain compliance with the standard.

SCOPE

According to the PCI-DSS, the following examples of system components may include, but are not limited to the following:

- Point of Sale Terminals and other credit card Point of Interaction (POI) devices facilitating credit card transactions.
- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including, but not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including, but not limited to, web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications that facilitate credit card transactions or enable integration with third-party payment providers.
- Any other component or device located within or connected to the CDE.

Fairfax County, as a defined merchant that accepts credit card transactions, is required to assess and report compliance with PCI-DSS on an annual basis. Assessment activities will include onsite visits, review of business procedures, staff interviews, and technical activities to ensure compliance with the standard is continuously maintained. **These activities are a shared responsibility between County Agencies, the Department of Finance, and the Department of Information Technology.**

The Department of Finance's Payment Card Acceptance Program also provides additional administrative guidance for Agencies in regard to the County's PCI-DSS program.

ROLES AND RESPONSIBILITIES

The following tables are intended to define the responsibilities expected of the Agency Merchants, Department of Information Technology, and the Department of Finance to achieve and maintain compliance in the use of secure technologies according to the PCI-DSS and for conducting annual assessment activities to validate continued compliance.

Agency Merchant Responsibilities
Ensure all acquired solutions are PCI Compliant, properly vetted through the DIT Architecture Review Board, and that actual technical implementation maintains compliance throughout the lifecycle.
Maintain current agency-specific network diagrams documenting the agency credit card processing environment and cardholder data flow. Updated diagrams must be submitted to DIT and DOF annually at a minimum, or upon any major change to the Agency environment.
Maintain a current agency-specific inventory of all systems in-scope for PCI compliance in the Agency's environment. This may include workstations, servers, credit card swipe devices, the assigned location for these devices, and the associated users of these systems. These inventory lists must be submitted to DIT and DOF annually for review.
Maintain a current list of all Agency users that have access to the payment processing environment and ensure restrictions are in place to limit access only to those defined users.
Ensure users complete annual security awareness training as provided by DOF and DIT. Agency users should receive training upon hire and annual refresher.
Ensure the accounts for users that are no longer working for the County are properly deactivated and that the user no longer maintain access to County resources.
Ensure the physical security of all Agency Point of Sale terminals (POS) and other in-scope systems or media in possession of the Agency, to include daily inspection for evidence of tampering.
Notify DIT and DOF of all changes to the Agency credit card processing environment that may impact the security of the systems and enterprise systems supporting the infrastructure.
Report all suspected incidents to DOF and DIT immediately.
Ensure all users are only processing credit cards on approved systems and according to approved compliant procedures that have been established for the credit card transaction environment. Credit card transactions should not be processed on systems in the Fairfax County internal network nor on systems that have not been previously approved for use.
Ensure Agency business procedures prohibit the use of sending or receiving credit card information through email and other messaging platforms.
Ensure any integration with third-party payment processors on public-facing web application used for card-not-present transactions fully and securely redirect to the third-party payment processor to minimize scope for compliance.
Ensure that all Agency acquired POS systems, applications, payment gateways, workstations, or other resources or services acquired for processing credit cards on behalf of the County are compliant with the PCI-DSS standard and that compliance is maintained by acquiring an annual Attestation of Compliance (AoC) from any third-party payment processors or service providers. Annual attestations received from third-party resources must be submitted to DOF and DIT for review as part of annual assessment activities.
Ensure the physical security of all systems and media throughout the lifecycle from creation to destruction.
Participate as needed in annual assessment and reporting activities which may include in-person and phone interviews, collaborating on the Agency self-assessment questionnaire (SAQ), and other compliance activities as required.

Department of Information Technology Responsibilities
Administer and provide security support for the dedicated virtual network established to segment Agency credit card processing environment from the internal County enterprise.
Administer the core network firewall securing the cardholder data environment (CDE) and receive and implement requests for changes from Agencies. Firewall rulesets will be reviewed quarterly.
Administer and use core network security tools and utilities, to include but limited to anti-malware, intrusion detection and prevention systems, to ensure the security of the CDE.
Ensure all DIT administered and owned applications, middleware, and operating systems that directly support or directly impact the security of the in-scope environment are current with all security updates and sufficiently hardened according to the PCI-DSS standard. All critical security updates must be applied within 30 days.
Administer the multi-factor authentication system required for non-console administrative access to the CDE.
Conduct at a minimum, quarterly network vulnerability assessments against in-scope Agency systems and coordinate with Agencies for remediation of any identified vulnerabilities as necessary.
Coordinate annual penetration testing activities against the network perimeter and in-scope credit card processing environment.
Assist with the completion and submission of the annual self-assessment questionnaire (SAQ) required for PCI-DSS compliance reporting for the programmatic areas that are administered and controlled by DIT.
Conduct an annual review of the IT Security Policy and this document which defines the technical requirements for integration of Agency acquired systems intended for credit card processing within the established dedicated network.
Maintain a current Incident Response Plan, as required by the standard, and lead technical response activities in the event of an incident.

Department of Finance Responsibilities
Review and select or approve merchant service providers and credit card payment gateway/middleware solutions through the county’s Department of Procurement and Material Management (DPMM).
Open, close, and maintain all merchant accounts and assist with enforcement and assessment of compliance with the PCI-DSS.
Coordinate with DIT for improving, modifying, expanding, and implementing technologies to enhance the Payment Card Acceptance Program throughout the County.
Coordinate annual PCI awareness training.
Update departments of periodic changes made by the card industry that affect the processing of card payments, industry trends, and technologies

TECHNICAL GUIDELINES FOR IN-SCOPE SYSTEMS

The following technical requirements are a shared responsibility between County agencies and DIT and may requirement enhancements to baselines established in the Fairfax County Information Technology Security Policy.

These technical requirements apply to all systems and applications that store, process or transmit cardholder information or host applications that are used to access or redirect to third-party payment providers or other payment solutions. Systems that are in-scope for PCI compliance may include, but are not limited to, Point of Sale Terminals (POS), network devices such as routers, switches and firewalls, and servers and windows computers.

Technical Guidelines for Systems and Applications
Fairfax County systems must not store credit card data to include un-redacted primary account numbers (PAN), magnetic stripe data, CVV code, or PIN. This includes, but is not limited to, servers, workstations, laptops, and other electronic media.
All swipe devices must be certified as P2PE or E2EE point of interaction (POI) devices. Card data should either be tokenized prior to transmission or validated to use a secure robust encryption transmission method as specified by the PCI-DSS council to send data to third-party payment gateways or other financial providers.
All vendor supplied default accounts and passwords must be changed before system installation.
All unnecessary default accounts must be removed or disabled before system installation.
All system components and software must be protected from known vulnerabilities by installing any applicable vendor-supplied security patches.
Critical security updates must be installed within one month of release for all system components.
All systems in-scope for PCI compliance must have anti-virus software deployed.
All users must be assigned a unique ID before allowing access to system components or cardholder data.
User accounts for terminated users must be immediately deactivated or removed.
User accounts must authenticate with a strong password of at least 7 characters with both numeric, alphabetic and special characters.
Group, shared, or generic accounts must be disabled or removed and must never be used for system administrative functions.

REFERENCES

Payment Card Industry Data Security Standard
Procedural Memorandum 70-05: IT Security Policy
FPS 241: Payment Acceptance Program