CHESTERFIELD COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES

Department:	**Information Systems Technology**	**Policy Number:**	**7-3**
Subject:	**Information Security Policy**	**Supersedes:**	**04/15/03**
		Date Issued:	**03/01/09**

I. INTRODUCTION

County employees regularly obtain, use and share information in the normal course of conducting the county's business. Electronic information collected, created, maintained, or transferred by county employees must remain accurate, complete and reliable through information-assurance processes for confidentiality, availability and integrity. Assurance may be accomplished through the assignment of system ownership, risk analysis, data classification, defined security roles and responsibilities, identification and authorization of system users, access control implementation of baseline-security measures in systems and guidance on appropriate handling of information in any media form or format.

A. Purpose

The purpose of this policy is to reduce information-security risks by defining necessary organizational information-security responsibilities and controls. The control goals to be achieved from information-security policies are to:

1. Assign formal responsibility for the integrity, safekeeping and dissemination of information
2. Assure compliance with statutory and regulatory requirements and/or county administrative procedures
3. Apply the information-security principle of "least privilege" by denying access to information without authorization from the information owner
4. Foster understanding of issues and necessary controls related to information security and privacy through information-security training and education
5. Ensure employee and system-user accountability for system activity through use of unique identification credentials and audit trails that monitor who performed a system activity
6. Report and reduce attempts of system misuse, abuse or other information security intrusions through logging, monitoring and violation reporting
7. Provide clarity of county expectations for information security
8. Promote continuity of business operations with timely detection and response to breaches of security, or other information-security incidents

B. Information-security control processes will be designed to:

1. Identify who is authorized to access information resources and under what conditions
2. Assess risk and identify cost-effective technical security safeguards
3. Maintain individual accountability and prevent unauthorized computer access

4. Protect organizational information and systems from malicious or inadvertent destruction, modification and/or disclosure
5. Prevent unauthorized disclosure, taking, copying, deleting or any other unauthorized use of computerized information
6. Provide incident response and monitoring of the environment to detect, correct and/or prevent information security threats
7. Communicate information security issues and responsibilities to the organization through information security education, training and awareness

II. DEFINITIONS

Data Owner
The *Data Owner* is the department head or designee responsible for the operation, maintenance and integrity of the data contained in a county IT System. The Data Owner is responsible for establishing the data's sensitivity, approving access to the data, and identifying storage, retention, and destruction guidelines in compliance with county records management procedures.

III. POLICY STATEMENT

Access to county systems, applications and information is restricted and is allowed only as necessary to support authorized business operations of Chesterfield County. The protection of computerized information assets must be in compliance with all applicable federal, state and local laws, ordinances and statutes.

It is the policy of Chesterfield County that each department head is responsible and accountable for the security of their organization's information (electronic, digital, or other computerized form) and for taking appropriate steps to secure the information by following county information security policies and procedures.

IV. RESPONSIBILITIES

A. Department Heads and Constitutional Officers

Each department or office who creates and maintains Primary Information of Record for a system is the Data Owner. As an owner of the information, the department or office is responsible and accountable to:

1. Promote the privacy and integrity of departmental information for which they have responsibility.
2. Classify the sensitivity or criticality of their owned information.
3. Understand and apply applicable laws, regulations, ordinances, statutes and/or county administrative procedures that govern the data owned by the department.
4. Communicate legal and regulatory compliance requirements for the department's data to the Information System Technology Chief Information Officer (CIO).
5. Authorize access privileges to the department's owned data.

6. Protect the department's owned data from unauthorized modification, destruction, disclosure and internal/external threats or any other misuse of the county systems and applications, whether intentional or unintentional.
7. Issue disclaimers as appropriate for data owned by the department regarding the accuracy or privacy requirements of information released.
8. Apply applicable controls to Public Access Stations in a manner to continue to allow availability of public information as required by law.

B. Information Security Steering Committee (ISSC)

The ISSC will:

1. Meet regularly to conduct the business of the ISSC
2. Prioritize major security initiatives across the county
3. Actively seek resources to accomplish the goals of the ISSC
4. Exercise confidentiality and discretion with regards to the content of the meetings and correspondence of the committee.
5. Address strategic countywide information security issues
6. Serve as an advisory board to the county administrator on an emergency basis, as the need arises
7. Maintain and protect the image of Chesterfield County
8. Maintain effective communications with the leadership group and departments
9. Monitor and update the information security strategic plan for the county
10. Ensure the information security strategic plan and security efforts are consistent with the county strategic plan
11. Initiate, review and recommend information security policies to the county administrator

C. Chief Information Officer (CIO)

The overall accountability to ensure enterprise-wide compliance and protection of all Chesterfield County electronic information assets resides with the county CIO. The CIO is responsible for directing appropriate countywide technical and information security control measures for enforcement of this policy.

D. Information Security Manager

The information security manager is responsible for implementing, managing and maintaining information security controls to ensure continuous operational support, protection and collaboration with learning resources to promote information security awareness.

E. Business Unit (Department/Constitutional Office) Information Security Representative

A business unit information security representative will be assigned for each business unit by the respective Department Head or Constitutional Officer. Access to electronic information for internal business unit personnel must be approved by the business unit Department Head or Constitutional Officer, or by the designated security representative for the business unit. A business unit security representative may not approve their own access privileges or those of a

director level or above. Access to non-public electronic information owned by another business unit must be approved by that business unit's Department Head or Constitutional Officer.

F. Information Systems Technology (IST)

IST will consult periodically with departments to determine necessary security and technical controls to protect all county electronic information. IST will also serve as a data custodian, utilizing appropriate security control measures to protect information in their custody for data processing purposes.

G. All County Employees

All county employees are responsible and accountable for ensuring the protection of their system and application account credentials that provide access to Chesterfield County computing environments. Employees will utilize safe computing habits and will not willfully abuse or misuse the computing services provided for the performance of their job duties for Chesterfield County government.

V. SEPARATION OF DUTIES

There are certain functions that must be separated physically in order to reduce the possibility of an individual taking advantage of that function, or to conspire to commit fraud or misappropriate resources. Basic internal control principles state that the same person should not initiate, authorize and enter a transaction. To support these necessary functional separations, the following restrictions should be observed:

A. Information system or application security roles (or profiles) will segregate system tasks as necessary to ensure an appropriate separation of duties is accomplished. Custody of an asset, record-keeping and authorization of the transaction should be separated. Example: Persons responsible for processing blank stocks of negotiable instruments should not have access to areas used for storage of these stocks. This would include checks, credit cards and all electronic transactions.

B. Departmental information security functions should be limited to a small number of individuals (such as a primary individual and a back-up individual) to ensure effective information security administration through appropriate separation of duties.

VI. RELEASE OF INFORMATION

Authorization to release Chesterfield County computerized information to private sector and public sector, internal and external organizations resides with the Data Owner. IST shall review the method by which the transfer is accomplished or the data is released. All county information identified as sensitive shall be encrypted during transfer to or in storage at an external organization.

A. Any contract that involves the release of electronic information from county systems and applications by IST to internal and external organizations must be approved by the Data Owner and the CIO prior to the release of the electronic information.

B. Any contract or agreement crafted for the purpose of facilitating the formal release of electronic information to external organizations via an IST approved data transfer process must be approved by the Data Owner.

VII. ENFORCEMENT

Misuse or Loss of Computer Resources – System risk assessment, access, authentication and authorization and continuity of operations control methods are required to prevent misuse or loss of computing resources. Monitoring and review efforts will be utilized to detect suspicious events. County disciplinary actions, including and up to termination, apply to all misuse or loss of computing resources.