Charles County Government
County Administrator Standard Operating Procedure

Title:	Information Technology Use and Security Policy	**SOP #:** CAP.FAS.04.001
Department:	Fiscal and Administrative Services	**Effective Date:** 8/2/2001
Division:	Information Technology	**Revision Date:** 4/27/2010 1/25/2011 7/24/2012 4/9/2013 12/15/2017
		Page 1 of 10
Purpose:	The purpose of the *Information Technology Use and Security Policy* is to: • establish procedures for the use of Charles County Government (County) technology tools and electronic data • protect the County, its employees and any authorized users of the County's technology tools from liabilities and service interruptions • protect the County's technology tools and information from security breaches, destruction and unauthorized distribution	
References:	Personnel Policy & Procedures Manual	
	Approved Cloud Applications List: https://icg.charlescountymd.gov/cloud-applications	

Procedure:

This policy documents the procedures that an authorized user must agree to follow in order to be provided access to the County's technology assets. Authorized users may be disciplined for noncompliance with this policy.

This policy does not purport to address every information technology operating and security issue. It is the authorized user's responsibility to use sound judgment. Should a user identify an issue or situation that is not addressed in this policy, they should consult their supervisor or contact the County Information Technology Division (IT) for guidance.

The *Information Technology Use and Security Policy* is subordinate to any employment contract or other employment agreements. The County may adjust this policy at any time.

Authorized users in non-exempt positions must adhere to the Overtime Policy (Chapter 14) detailed in the Charles County Personnel Policy and Procedures manual.

Please read the policy carefully and sign the "Information Technology Use/Access Release" form attached. The signed form should be returned to IT.

1.0 DEFINITION

Information Technology is defined as any equipment, or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Technology Assets are defined as all hardware, software, networks, data, automation services, tools or devices owned by or licensed to Charles County Government and available for Charles County Government's "official use" in its Information Technology needs.

Technology Assets include, but are not limited to, desktop computers, laptop computers, terminals, mobile devices, telecommunications equipment and all related peripheral equipment and software. County technology assets also include voice mail, Internet connectivity, County owned or licensed software applications, email, and all County data and information, regardless of where it is stored.

An **Authorized User** is defined as any individual who has been authorized to use County technology assets. Authorized users have reviewed and signed the Information Technology Use/Access Release form. An authorized user could be either a full-time or part-time County employee, or a non-employee who has been granted authority to access County technology assets.

The **Cloud** is a network of remote servers hosted on the Internet and used to store, manage, process, and transfer data.

A **Cloud Service Provider (CSP)** is a company which provides data storage, network services, infrastructure, or business applications in the cloud. This includes any company which stores the County's data offsite. Common examples include: Microsoft Office 365, Amazon Web Services, Facebook, Salesforce, etc.

Cloud Services include any application or service provided to a customer that is hosted on a CSP's infrastructure.

Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information. Each category of information used by the County requires a case-by-case assessment of the specific risk that an individual can be identified. Be aware that non-PII can become PII whenever new information is made available, and can be linked to the preexisting information to identify an individual.

2.0 GENERAL GUIDELINES

a. <u>Unacceptable Use</u>

Under no circumstances is an authorized user permitted to engage in any activity that is illegal under local, state, federal or international law while utilizing County technology assets.

The following activities are, in general, prohibited when utilizing County technology assets:

- Violations of the rights of any person, company or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Charles County Government.
- Unauthorized copying, redistributing or republishing of any copyrighted material including, but not limited to, photographs from magazines, books or other copyrighted sources, music, data, software, manuals, etc.
- Intentionally introducing malicious objects (software, malware, viruses, etc.)
- Any action where the intent is to maliciously disrupt Charles County Government's, or another user's, technology tools.
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Effecting security breaches. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a system or account to which the user is not expressly authorized to access.
- Circumventing user authentication or security of any technology asset.
- Distribution or use of profane or obscene language/graphics.
- Personal financial gain, commercial activity or to operate a business.
- Storing PII in unauthorized locations. The unauthorized dissemination of PII.

An employee's use of County technology assets for any of the above may be grounds for dismissal, may result in loss of access to County technology assets and/or may invoke other disciplinary actions as described in the Charles County Personnel Policy and Procedure Manual, Chapter 10, Disciplinary Actions.

A non-employee's use of County technology assets for any of the above may result in loss of access to County technology assets and/or may invoke legal action.

b. <u>Inappropriate Use</u>

Authorized users are expected to conduct themselves professionally in the workplace and refrain from using County technology assets for activities that are inappropriate. Misuse or inappropriate use of County technology assets includes, but is not limited to:

- Any use that could cause congestion, delay, or disruption of services to any Charles County IT technology tools, for example, sending mass emails with large file attachments, streaming personal video services (e.g. Netflix), non-business use of file sharing, etc.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Posting County information to external newsgroups, bulletin boards, social media or other public forums without authority.
- Any use that could generate additional expense to the County without prior management approval.

c. Acquisition of Technology Assets

IT is responsible for maintaining the County technology assets, such as networks, desktop computers, servers, printers, peripherals, mobile devices, software, and cloud services, as well as ensuring that these technology assets are acquired and maintained at reasonable costs.

All technology assets must be purchased by IT or, in unique cases, after consultation with IT. This process is intended to provide:

- a centralized point of information regarding technology assets
- a County wide inventory of hardware and software
- pricing advantages
- software license compliance
- software media storage and management
- hardware and software integration/compatibility assurance

d. IT Work Request System

Authorized users must utilize the IT Work Request System to request IT services or equipment.

e. Personal Use

County employees are permitted use of County technology assets for personal needs if the use does not interfere with official business and involves no additional expense to the County. No additional expense means that an employee's personal use of County technology assets is limited to those situations where the County is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the County.

This personal use of County technology assets should take place only during the employee's non-work time.

This privilege to use County technology assets for personal needs may be revoked or limited at any time by this policy or departmental management. Privilege means, in the context of this policy, that Charles County Government is extending the opportunity to its employees to use County technology assets for personal use in an effort to create a more supportive work environment.

This privilege does not create a right to violate any of the items detailed in this policy.

f. Protect Your Computer Equipment

All authorized users share in the responsibility to protect County technology assets from physical and environmental damage, loss and theft. Users are responsible for the correct operation and physical security of the County's technology assets. Destruction, theft, alteration, or any other form of sabotage of County technology assets is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Authorized users must immediately notify IT in writing if any technology asset assigned to them has been damaged, lost or stolen.

g. Use Only Approved Software

Software installed on and/or used by County desktop/laptop computers must be approved and installed by IT. IT will maintain all County approved software media, licenses and documentation. Only IT approved and installed programs/systems may be used by authorized users on County desktops/laptops.

County licensed software may only be reproduced by IT personnel in accordance with the terms of the software licensing agreements.

h. Computer Hardware Configuration Changes

Only IT can authorize configuration changes to any computer hardware. Only IT personnel can install or replace technology related hardware.

i. Protect Your Password

Do not share your password with anyone; this includes supervisors and IT support personnel. Do not write it down where someone can find it. Do not send it over the Internet, email, instant message or SMS text without an acceptable encryption technology. Select complex passwords.

Users will be held accountable for activity performed under their credentials.

j. Protect County Information

Desktop, laptops and tablets shall not be left unattended whereby inappropriate access to County owned and/or held information may be gained by unauthorized persons. Authorized users should restrict access to their assigned technology assets when leaving their work-area. Authorized users should shut down their PCs at the end of their work day.

k. Guard Against Computer Viruses

Authorized users shall virus scan all files which are downloaded from the Internet or brought in on removable media. IT provides current anti-virus scanning software to allow users to perform this task. It is the user's responsibility to make sure that they understand how to use the anti-virus scanning software.

Authorized users who are issued County laptops and tablets are required to connect to the Charles County Government network on a monthly basis. When a laptop is connected to the network, the latest anti-virus and system updates are automatically downloaded.

l. File Security

Various programs allow authorized users to password protect or encrypt individual files. Upon request by the authorized user's management, an IT employee or prior to separation of employment with Charles County Government, users must remove a password from, or provide decryption for, any such files.

m. Information Security Awareness Training

Authorized users must complete the County's online Information Security Awareness Training on an annual basis. The purpose of the training is to educate employees about information

security awareness and provide best practices to help ensure the protection of County technology assets from unauthorized use. Authorized users will receive automated emails when they are due to take the IT Security Awareness Training.

2.1 County Information and Data

a. Ownership

Charles County Government shall own all rights, title, and interest in its information and data regardless of where it is stored.

b. PII

Authorized users must follow all applicable laws and regulations concerning the use and protection of all PII to which they have access.

c. Storage and Protection

Authorized users are responsible for the protection of essential data files and the security of County information. Storing files and information on the desktop or laptop computer hard drive, a mobile device, or in the cloud, does not ensure protection or security of the information. IT does not backup desktop or laptop computer hard drives, mobile devices or information stored in the cloud.

- All County information must be stored on the Charles County Government network (CCGNET) or an authorized CSP's infrastructure. PII shall not be uploaded to a CSP's infrastructure, unless the CSP is approved specifically for storing PII.
- CCGNET is equipped with electronic and physical security. Activity on CCGNET is monitored for tampering and other security breaches. Maintenance and back up are performed on CCGNET regularly. Programs and other information are updated on CCGNET as necessary.
- It is the authorized user's responsibility to make sure that they understand how to use CCGNET and other County authorized information storage locations.

2.2 Electronic Mail (Email)

Authorized users should use the County's email system when conducting County business electronically.

a. Only Essential Email Should Be Saved

Employees should only retain email that is of importance. Non-essential email should be disposed of once it's acted upon.

b. Archiving

Archiving is a means to move messages (mail, tasks, appointments, notes, and phone messages) to a specified directory on a network server, reducing the burden of messages which the email system must manage. Authorized users should archive email regularly.

c. Spam

The County email system should not be used for the distribution of email chain letters. The County email system should not be used for the distribution of spam (unsolicited commercial email, including non-approved fund-raisers, chain letters, hoaxes, etc.).

d. Malicious Email

Malicious email and links are methods used to harm the recipient in some way. Never respond to an email asking for personal or financial information. Never click on a link or a file/attachment within an email from someone you do not know or trust. Report all 'suspicious' email by forwarding the email, as an attachment, to emailabuse@charlescountymd.gov

e. Use Email as Appropriate

Email can be a powerful, productive and time-saving tool when properly used. It is not however, a substitute for other necessary and appropriate forms of communication.

When improperly used, email can unnecessarily absorb valuable time and personal resources by requiring the daily review of large numbers of messages which may be unnecessary or more appropriately conveyed through face-to-face communication.

Email should not be used to communicate PII.

Email does not absolve the sender of necessary and appropriate verbal or in-person follow-up responsibility.

f. Mass Email

A mass email is one that is sent to a large number of recipients.

- Departments should be extremely judicious in sending unsolicited email to the "All CCG" group. "All CCG" directs mail to everyone on the County email system.
- If any mass email, including "All CCG" email, requires an attachment, the attachment should be posted to either the County's Intranet site (ICG) or the County's Internet site (www.charlescountymd.gov), and the email should contain a link to the attachment, not the actual attachment itself.
- Department Heads should review "All CCG" emails originating from their department before the message is sent.
- Anyone sending a mass email must include his/her email address, telephone number and departmental affiliation in the message so that recipients can easily identify the sender.
- When sending a mass email, place all of the addresses in the blind carbon copy (BC:) field of the message to protect the privacy of the recipients.
- Departments that send frequent or regular mass mailings are encouraged to maintain their own groups. Emails to these groups should include instructions as to how a recipient can opt out of future mailings.
- Keep mailing groups/lists current.
- When replying to a mass email, avoid using the 'Reply All' option. Instead, select 'Reply' to reply only to the sender and avoid spamming all of the other recipients.
- When establishing automated email rules, never choose an option that would result in sending an email to a large mailing list, including "All CCG".

2.3 Internet

a. Internet Use/Access
Internet use/access is for official Charles County Government business except as provided for in 2.0(e).

b. List Server/Mailing List Subscriptions
Authorized users will not subscribe to any non-work related list servers or mailing lists without prior Department Head authorization.

c. Inappropriate Website Access
Authorized users will not access violent, pornographic or other inappropriate websites through the Internet. Authorized users will not access any chargeable website without prior Department Head authorization.

Charles County utilizes Web Filtering software to block access to inappropriate internet sites on County government computers. Should an authorized user need access to a blocked site, the request should be made via the IT Work Request System and approved by the Department Head.

2.4 Cloud Services

a. Cloud Services Use/Access
Use only approved and managed CSPs.

- Authorized users shall only use CSPs that have been approved for County business use by the Department of Fiscal & Administrative Services, Information Technology Division.
- Authorized users shall only use County approved user accounts to access a CSP's infrastructure for County business use. The use of unapproved user accounts to store County owned information is not permitted.
- Authorized users shall only use County approved methods or tools to access a CSP's infrastructure for County business use.

b. Approved CSPs
Please refer to https://icg.charlescountymd.gov/cloud-applications for a list of all County approved CSPs.

2.5 Violations
Misuse of Charles County's technology assets or breaches of IT security is a violation of this policy and may result in disciplinary action, up to and including termination of employment.

2.6 Separation of Employment
Upon separation of employment from Charles County, all County-owned IT equipment provided to an authorized user must be returned in good and usable condition no later than the last day of employment. If the equipment is not returned or is returned damaged and unusable, the cost of

replacing the equipment will be withheld from the employee's final paycheck under the terms of the federal Fair Labor Standards Act (FLSA).

As detailed in the File Security section (2.0(l)), prior to separation of employment with Charles County, authorized users must remove passwords from any County files and decrypt any files which they have encrypted.

3.0 POLICY ADMINISTRATION AND REVIEW

3.1 Administrator Access and Monitoring

All files on County devices or networks (including email) and all phone records of County-owned telephones are the property of Charles County Government. Authorized users understand that they do not possess a "right to privacy" in County email or phone communications.

An IT Administrator may access authorized users mailboxes, telephone records or network activity for any valid administrative purpose, including, but not limited to, the following:

1. To retrieve lost messages,
2. To recover from system failures, or
3. To monitor system performance.

At the direction of the County Administrator or Deputy County Administrator, an authorized user's email, internet usage, network activity or telephone records may be monitored for any valid business-related purpose, including, but not limited to, investigation of the following:

1. Excessive personal use,
2. Violation of federal, state or local law, or
3. Personnel issues or violation of County policy.

3.2 Legal Compliance

Information and communications pertaining to County business constitute public records under the Maryland Public Information Act ("MPIA") and may be subject to disclosure. Such information and communications may also be subject to discovery in the event of litigation involving the County.

To comply with any applicable legal requirement, IT Administrators may access email mailboxes, network files or telephone records at the direction of the County Administrator, Deputy County Administrator, the County Attorney, or an Associate County Attorney.

3.3 Supervisor and Department Responsibilities

a. Monitoring Usage

All supervisors within the County departments are responsible for ensuring that their authorized users are aware of, and adhere to, these policies and procedures.

b. Notifying IT

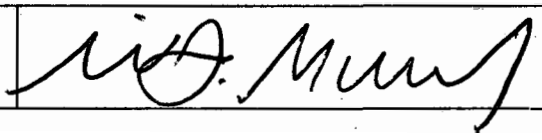
Departments are responsible for providing notification to IT via the IT Work Request System when an authorized user begins, changes or ends employment with Charles County Government. If a department requires the immediate termination of an authorized user's access to County technology assets, the appropriate departmental representative should notify IT by phone and then document the request via the IT Work Request System.

c. Information Technology Use/Access Release form

A signed Information Technology Use/Access Release form must be received in IT prior to granting access to IT systems.

4.0 EXCEPTIONS

Provisions of this policy may be waived at the discretion of the County Administrator. Any and all exceptions to this policy must be approved in advance.

Authorized:		**Date:** 12-15-17