FULTON COUNTY

POLICY AND PROCEDURE

SUBJECT: **Information Technology-Acceptable Use Policy**

DATE: March 21, 2012	NUMBER: 600-60

STATEMENT OF POLICY

The purpose of this Information Technology (IT) Acceptable Use Policy is to summarize focus points of the County's IT security guidelines and confirm that authorized users are aware of these rules by their acknowledgment of this policy. Information Technology resources are provided to authorized "users" to conduct and facilitate official County business. It is the responsibility of each user to make certain that such resources are not misused. This policy summarizes user responsibilities and governs the acceptable use of IT infrastructure, services, and equipment. The Department of Information Technology (DoIT) must approve all IT related purchases including services and goods. All IT related equipment must conform to IT standards and protocols. DoIT will not support any equipment or services that do not comply with IT standards. All information created, transmitted, and stored on Fulton County IT resources are the sole property of Fulton County and is subject to monitoring, review, and seizure. All requests for public records are to be coordinated through the Fulton County Attorney's Office pursuant to County Policy 600-10 (Implementation of Georgia Open Records Act), before access is granted to the public.

The acceptance and use (i.e. authentication) of County provided system "logins" (username + password) is an acknowledgement of all IT policies. The failure to sign any form(s) required by Fulton County to access or utilize its IT system will not absolve or prevent you from being disciplined or being subject to civil or criminal prosecution from its misuse. The County may institute additional, supplemental or new policies subsequent to this agreement to better define specific categories relating to IT resources. Failure to comply with IT policies and procedures may subject a user to County and agency-specific disciplinary action. In addition, a violation of this policy may also be a violation of the law and could subject a user to an investigation and criminal or civil prosecution.

APPLICABLITY

This policy shall apply to all Fulton County users including: employees (permanent, temporary, contract), officers, elected officials, consultants, vendors, etc. For the purposes of all IT policies and procedures, the term "user" refers to anyone who is provided access to the County's IT resources such as infrastructure, services or equipment.

POLICY OVERVIEW

The following are key points regarding the use of IT resources and IT security:

- Information created or used in support of County business activities is the property of the County.

- Users have no privacy rights, except those that may be afforded by State of Georgia or federal laws, when using County resources and/or equipment.
- Assigned IT resources are meant to facilitate the efficient and effective performance of official duties. It is each user's responsibility to ensure that these resources are not misused and that they comply with all laws, County policies and procedures.

- All requests for IT service and equipment should be directed to the IT Service Desk using the following options:
  - Telephone- (404) 612-7334 (Use phone option for after-hours emergencies to engage the on-call staff)
  - Email- helpdesk@fultoncountyga.gov
  - Online- self-service requests can be made via the Employee Portal

- Users will accept financial responsibility for replacement or repair of IT assets in their possession as a result of neglect and/or misuse. Fulton County Personnel Regulations 1800-11-C and 1800-11-D, among others, govern the disciplinary actions associated with the misuse of County owned assets by employees.

- Many County facilities house sensitive or critical information systems. You are expected to comply with all physical access controls designed to restrict unauthorized access.

- It is the responsibility of each user to take appropriate precautions to prevent damage, loss, theft and unauthorized use of their County-issued equipment. Locking devices and strong passwords should always be used to minimize theft and unauthorized use.

- The use of the IT network and Internet is a privilege, not a right. If you violate any applicable policy, you may lose your access. The County may refuse to reinstate your access. The County may also take other disciplinary action.

- Users must return all issued IT assets to their supervisor or department head upon transfer, termination, retirement, or any form of separation from the County. Examples of IT assets include (but are not limited to) computers, laptops, printers, projectors, scanners, cameras, phones, radios, pagers, software or other applications, any data stored on any media including file servers, portable storage media, etc. Failure to return these assets will result in appropriate action being taken by the County.

USER RESPONSIBITIES

User responsibilities fall under several categories. Each category and the key responsibilities associated with it are listed below:

USER IDs AND PASSWORDS

- You will be issued a network username/userID/logon unique to you. Only you may use your userID to access County resources (e.g. computer, telephone, software applications, etc.).

- You will be issued a default password at the same time as your userID. You will be immediately prompted to change your password the first time you login to the network/system.

- Users must use strong passwords (as defined herein) and will be required to change their passwords frequently for security purposes.

- Do not share your userID + password with anyone including coworkers and/or supervisors. Treat your password as sensitive and highly confidential information.

- Change your password immediately if you think someone else knows it *(CTRL+ALT+DEL, Change Password)*. Report your suspicions to management and the Department of Information Technology (DoIT).

- If you lose or forget your password, *you* will need to request a password reset through DoIT. No one else can do it for you.

- All mobile devices, including smart phones, tablets, etc. must be configured with password protection that activates after two (2) minutes of idle time to minimize unauthorized use.

- Use the "logoff" or "lock" feature with password protection anytime you leave your workstation (especially remote sessions) to minimize unauthorized use.

HARDWARE AND SOFTWARE

- Never download or install any software to any County device without prior written approval from the Department of Information Technology (DoIT).
- Any costs/fees associated with unauthorized downloads or services will be the user's responsibility (e.g. downloads from mobile "Apps." markets/stores).

- Do not make any changes to system and/or software configuration files unless specifically authorized in writing by DoIT.

- Do not connect a laptop or any other mobile device to the County's secure network until it has been approved by DoIT and scanned for viruses and malicious software.

- Follow the authentication procedures defined by DoIT whenever you login to the County's network via a DoIT approved remote access protocol.

- Retain original software installed on your computer if it is provided to you. The software must be available when your system is serviced in case it needs to be reinstalled.

- Do not keep liquids or magnets on or near computers, as they can cause serious damage.

- Report all IT systems problems in detail on the appropriate form and/or when you contact the DoIT Help/Service Desk or discuss the problem with your agency's IT Coordinator.

- Report equipment damage and/or loss immediately to the DoIT Help/Service Desk and your department head.

EMAIL and TELEPHONE

- County email, telephone systems and networks are to be used for official County business.
- Email is provided to employees for the administrative needs of the County. Email correspondence to/from a County email account is considered public information and may be subject to release under the Georgia Open Records Act (OCGA 50-18-70 et seq.) or pursuant to subpoena. All requests for public records are coordinated through the Fulton County Attorney's Office pursuant to County Policy 600-10-Implementation of Georgia Open Records Act.
- Management can freely inspect or review email and data files including voicemail. Employees should have no expectation of privacy regarding their Internet usage, email or any other use of County computing or telephone device.

- Do not use a County email account or voicemail box assigned to another individual to send or receive messages unless you have been authorized in writing by your department head to act as that individual's delegate.

- Use of personal Internet-based (external) email systems from County networks is prohibited unless there is a compelling business reason for such use and prior written approval has been given by DoIT.

- Do not configure or use automated forwarding to send County email to Internet-based (external) email systems unless specifically authorized to do so, in writing, by DoIT.

- Send confidential information via email only with the written permission of your department head and only via an approved encryption method. Mark the email according to agency retention policies.

- Treat confidential or restricted files sent as attachments to email messages as *highly sensitive information*. This also applies to confidential or restricted information embedded within an email message as message text or a voicemail message.

- Do not delete any records (e.g. email, voicemails, etc.) if management has identified the subject matter as relevant to pending or anticipated litigation, personnel investigation, or other legal processes.

- Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.

- Broadcast e-mail messages are to be coordinated centrally by an approved member of the County's Office of Communications and using a DoIT approved ListServ. service and are not to be sent by individual users using County email.

INTERNET / INTRANET

- Internet/Intranet access is to be used primarily to conduct County business.

- You may access the Internet for limited personal use only during non-working time and in strict compliance with IT policy. If there is any doubt about whether an activity is inappropriate, consult with your department head, his/her designee or DoIT.

- Fulton County offers unsecure Public WiFi Internet access at a number of facilities for use by constituents who visit a County facility to conduct business. Use of Fulton County's unsecure Public WiFi Internet access by employees who have been provided access through the secured wired or wireless network is strictly prohibited, unless authorized in writing by DoIT.

INFORMATION SECURITY

- Treat hardcopy or electronic Personally Identifiable Information (PII) as confidential and take all precautions necessary to ensure that it is not compromised. Intentional or even accidental disclosure of PII or other security sensitive data to unauthorized users is a violation of policy.

- Official emails and Systems Alerts from Fulton County DoIT will always have the following:
  - DoIT Systems Alert Header
  - @fultoncountyga.gov address
  - Or come directly from the Chief Information Officer (CIO)

- Don't leave PII or sensitive information unattended or unsecured for any period of time.

- Be sure to follow your agency's policy for disposing of confidential/sensitive data. This may include the physical destruction of data through shredding or other methods.

- Confidential or sensitive data should never be stored locally (i.e. hard drive of any device) on any remote endpoint device without written approval from your department head and proper security/encryption applied. All sensitive data should be stored on the County's secure data network.

- Confidential or sensitive data should never be sent via email without the proper data encryption applied. If there is a business need to send sensitive data via email, the department head may request encryption services through DoIT for named users.

- Maintain your business data files on the County's secure data network or "shared" network drive (e.g. H:, P: drives) so that they can be backed-up according to DoIT's

regular back-up schedule. Data on local hard drives (e.g. C: drive, portable storage, etc.) are not backed-up by DoIT and may be lost in the event of a hardware failure.

- Storing confidential or sensitive data to "cloud" storage services (e.g. Google Cloud, iCloud, etc.) or any unauthorized data network is strictly prohibited.

- All users are responsible for ensuring proper retention of data/records in compliance with law and agency-specific records retention schedules. This includes all records created and stored using IT resources. Please consult your department head to ensure you understand your agency-specific records retention schedules. Data/records with no retention value and that do not contain sensitive information should be archived off the County's secure shared data network.

- Remote access to the County's secure network must be approved by your department head and DoIT. DoIT defines all remote access protocols and tools. Unauthorized remote access accounts (e.g. personal GoToMyPC, LogMeIn, etc.) are strictly prohibited and may lead to the revocation of IT access and disciplinary action.

- All individuals and machines, while using the County's remote access technology, including County-owned and personal equipment, are a de facto extension of Fulton County's secure network, and as such are subject to the County's IT Acceptable Use Policy and IT security checks.

- All devices (e.g. computer, cell phone, tablet, etc.) connecting to the County's network must be approved by DoIT and will be subject to IT security protocols. At minimum, all remote computers must maintain up-to-date operating systems with security patches and up-to-date anti-virus software; this includes all personally-owned devices. Antivirus software is available for authorized remote users.

- Never use a public PC (e.g. Internet Café, Kinkos, etc.) or any unsecure end-point device to remotely connect to the County's secure network. Hackers will often install malicious software such as keystroke loggers to obtain confidential/sensitive information.

- Lost devices (which have been connected) must be reported to DoIT and may be subject to remote erasure/wipe to minimize unauthorized use and potential security breaches. Personal data may be lost.

- Users must use "https:" (i.e. hypertext transfer protocol secure) on any website where authentication (i.e. username + password) and/or security sensitive information is passed (e.g. payment transactions, etc.)

- IT security standards and protocols are designed to minimize the potential exposure to Fulton County from damages which may result from unauthorized use of the County's resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical County internal systems, etc.

- Information created, sent, stored or received via the email system, network, Internet, telephones (including voicemail), fax or the Intranet is the property of the County.

- Do not expect information you create and store on County systems, including email messages or electronic files, to be private. Encrypting or using other measures to protect or "lock" an email message or an electronic file does not mean that the data are private.

- The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary.

- The County may disclose text or images to law enforcement without your consent as necessary.

ADDITIONAL PROHIBITEDED ACTIVITIES

Unless you are specifically authorized by your department head and DoIT in writing, the following uses are also prohibited (Violators will be disciplined under appropriate Fulton County regulations or as provided by other applicable civil or criminal laws):

- Using, transmitting, or seeking inappropriate or offensive materials, including but not limited to vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.

- Accessing, attempting to access, or encouraging others to access inappropriate or offensive materials, including but not limited to vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory language or materials.

- Revealing confidential/sensitive or PII without permission, such as another's home address, telephone number, credit card number, Social Security Number, medical records, etc.

- Making offensive or harassing statements and/or jokes which violate EEO policies concerning but not limited to language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

- Sending or soliciting sexually oriented messages, images, video or sound files.

- Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.

- Gambling or engaging in any other activity in violation of local, state, or federal law.

- Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:

    - Accessing, transmitting, or seeking confidential information about clients or coworkers without proper authorization.

- Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others.
- Knowingly downloading or transmitting confidential information without proper authorization.

- Uses that cause harm to others or damage to their property. These include but are not limited to the following:

  - Downloading or transmitting copyrighted materials without the permission of the copyright owner (e.g. music, movies, files, etc.) Even if materials on the network or the Internet are not marked with the copyright symbol, ©, assume that they are protected under copyright law.
  - Using someone else's password to access the network or the Internet.
  - Impersonating another user or misleading message recipients into believing that someone other than the authenticated user is communicating a message.
  - Uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network.
  - Creating, executing, forwarding, or introducing computer code designed to self-replicate, damage, or impede the performance of any computer's memory, storage, operating system, application software, or any other functionality.
  - Engaging in activities that jeopardize the security of the County network or other networks on the Internet.

- Conducting unauthorized business or commercial activities including, but not limited to:

  - Buying or selling anything over the Internet.
  - Soliciting or advertising the sale of any goods or services.
  - Unauthorized outside fund-raising activities, participation in any lobbying activity, or engaging in any prohibited partisan political activity.
  - Posting County, department and/or other public agency information without permission from you department head to external news agencies, service bureaus, social networking sites, message boards, blogs or other forums.

- Uses that waste resources, including, but not limited to:

  - Printing of personal files.
  - Sending chain letters for any reason.

Departmental Sponsor:

Department of Information Technology (DoIT)

Policy Review Date:

March 2013

References:

- Georgia Open Records Act, as amended, O.C.G.A. § 50-18-70 et seq. and Fulton County Code § 102-81
- Policies and Procedures 600-10- Implementation of the Georgia Open Records Act
- Fulton County Personnel Regulations 1800-11-C and 1800-11-D
- Policies and Procedures 600-61- IT Network Infrastructure Administration

Departments Affected:

All County Users

TERMS AND DEFINITIONS

Authentication	The process of verifying the identity of anyone who wants to use County information systems before granting them access. Also know as "login" (username + password).
Back-up	To copy files to a second storage medium (for example, a disk or tape) as a precaution in case the first storage medium fails.
Confidentiality / Non-Disclosure Agreement	An agreement that outlines sensitive materials or knowledge that two or more parties wish to share with one another. They agree not to share or discuss with outside parties the information covered by the agreement.
Configuration Files (System or Software)	Highly important files that control the operation of entire systems or software.
Copyrighted	The legal right granted to an author, composer, developer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.
DoIT (Department of Information Technology)	Fulton County agency responsible for IT resources such as technology infrastructure/networks, applications/software and data systems.
Electronic Communication	Messages sent and received electronically through any electronic text or voice transfer/storage system. This includes e-mail, text messages, instant messages (IM), voicemail, etc.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to "*decrypt"* it. Unencrypted data is called *plain tex*t; encrypted data is referred to as *cipher text*.
Hacker	Person who accesses a computer system by circumventing its security system.
Information Security	Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
Information Technology (IT)	The broad subject concerned with all aspects of managing and processing information within an organization.
Keystroke Logger	Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
Listserv.	Email service which allows large broadcast emails to be sent without compromising the County's internal email systems.

Local Security Administrator (LSA)	The person at each agency who is responsible for the operational maintenance of IT security resources within the agency.
Malicious Software	Malware, short for malicious software, is software (or script or code) designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.
Network	Two or more linked computer systems. There are many different types of computer networks.
Password	Sequence of characters (letters, numbers, symbols) used in combination with a User ID/username to access a computer system or network. Passwords are used to authenticate the user before s/he gains access to the system.
Personally Identifiable Information (PII)	Any piece of information that could be used to uniquely identify, contact, or locate a single person. Examples include: full name; national identification number; email address; IP address; driver's license number; and Social Security Number.
Portable Storage Device	Any device used to store data/information that can be carried from one place to another with relative ease.
Records Retention	Retention requirements is a term used to refer to the rules set by the State of Georgia regarding the length of time different types of public records must be stored before they can be discarded.
Remote Access	Accessing the County's secure IT network from a remote location outside of the County's corporate firewall (e.g. home, field, etc.). Remote access services are defined by DoIT (e.g. VPN, Remote Desktop Protocol, etc.)
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which would adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.
Strong Passwords	A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed.
User	Any individual who is provided access to the County's IT resources including employees and contractors.
UserID	Unique name given to a user for identification to a computer or telephone network, database, application, etc. Coupled with a password, it provides a minimal level of security.
Virus / Malicious Software	A software program that interferes with computer operation, damages or destroys electronic data, or spreads itself to other computers. Viruses and malicious software are often transmitted via email, documents

	attached to email, and the Internet.
WiFi	Any of several standards for short-range wireless data transmission.
Workforce Member	Any member of the County workforce, including employees, temporary help, contractors, vendors and volunteers.

ACKNOWLEDGEMENT

- If you disregard security policies, standards, or procedures, you are subject to County and agency-specific disciplinary action.
- A violation of this policy may also be a violation of the law and could subject you to investigation and criminal or civil prosecution.

By signing this document, I acknowledge that I have read, understand and will comply with the Fulton County Information Technology Acceptable Use Policy. In addition, the acceptance and use (authentication) of County provided system "logins" (username + password) is a further acknowledgement of all IT policies. I understand that there are additional and may be subsequent IT related policies that will be available for me to review.

USER INFORMATION

Last name	First name	Middle

DEPARTMENT OR COMPANY INFORMATION

Department or Company Name	Division

Date	**User Signature**
	X_____

Cc: Employee Personnel File
Contract File