FULTON COUNTY

POLICY AND PROCEDURE

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

DATE: April 21, 2010	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 County may institute additional, supplemental or new policies subsequent to this agreement to better define specific categories relating to IT resources. 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 in compliance with the Georgia Open Records Act, as amended, O.C.G.A. § 50-18-70 et seq. and Fulton County Code § 102-81.

All staff must sign this agreement upon entry into the County indicating that they understand and will comply with all IT policies and procedures. In addition, the acceptance and use (authentication) of County provided system "logins" (username + password) is a further acknowledgement of all IT policies. 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 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 IT resources and security:

- Information created or used in support of County business activities is the property of the County.
- Users have no privacy rights 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 IT policies and guidelines.

- Users must abide by all policies governing the use of Fulton County assets. 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 govern the disciplinary actions associated with the misuse of County owned assets.

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

- The use of the IT network and Internet is a privilege, not a right. If you violate 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 termination, retirement, or separation from the County. Typical IT assets are desktops, laptops, cellular phones, BlackBerrys, pagers, radios, access cards, software, memory drives, tools and test equipment.

USER RESPONSIBITIES

User responsibilities fall under several different IT 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 log into the system.

- Do not share your userID and password with other users or individuals, 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.

HARDWARE AND SOFTWARE

- Never download or install any hardware or software without prior written approval from the Department of Information Technology (DoIT).
- Do not make any changes to system and/or software configuration files unless specifically authorized in writing by DoIT.
- Maintain your business data files on a network or "shared" drive (e.g. H: or P: drive) so that they can be backed-up according to DoIT's regular back-up schedule. Data on local hard drives (e.g. C: drive) are not backed-up by DoIT.
- Use the "logoff" feature any time you leave your workstation.
- Do not connect a laptop or other mobile device to the network until it has been scanned for viruses and malicious software.
- Follow the authentication procedures defined by DoIT whenever you login to the County network via Remote Access.
- Do not attempt to connect your workstation, laptop, or other computing device to the Internet via an unauthorized wireless or other connection.
- 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 computer 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 or your agency's IT Coordinator.

EMAIL and TELEPHONE

- County email, telephone systems and networks are to be used for official County business.
- 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 equipment.
- 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, 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 agency management and 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 management and only via an approved encryption method. Mark the email according to agency policy.

- 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 email, voicemail messages or any other data if management has identified the subject matter as relevant to pending or anticipated litigation, personnel investigation, or other legal processes.

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.

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 to unauthorized users is a violation of policy.

- Don’t leave PII unattended or unsecured for any period of time.

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

- 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.

PROHIBITED ACTIVITY

Unless you are specifically authorized by your department head and/or DoIT in writing, the following uses are prohibited:

- 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 PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.

- 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.

- Downloading or using any software on the network other than those which are licensed and approved by the County.

- 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 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.
  - Including unnecessary recipients on an email. Only copy others on an email or voicemail message who should be "in the loop" on the topic addressed.
  - 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 Communications Department and are not to be sent by individual users..

Departmental Sponsor:

Department of Information Technology (DoIT)

Policy Review Date:

April 21, 2010

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.
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*.
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.
Local Security Administrator (LSA)	The person at each agency who is responsible for the operational maintenance of IT security resources within the agency.
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.
Remote Access	Accessing the County's secure IT network from a remote location (e.g. home, field, etc.) using DoIT approved access service (e.g. VPN, Remote Desktop, etc.)
User	Any individual who is provided access to the County's IT resources such as infrastructure, services or equipment.
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.
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. I understand that there are additional and may be subsequent IT related policies that will be available for me to review.

EMPLOYEE INFORMATION

Last name	First name	Middle

DEPARTMENT INFORMATION

Department Name	Division

Date	**Employee Signature**
	X_____

Cc: Employee Personnel File