Electronic Communications and Security Policy

Effective Date: Adopted 10/25/2005

§-I. PURPOSE
To authorize the Information Services Department to promulgate and communicate Information Technology Security Standards (Security Standards) concerning the use, protection, and preservation of computer information systems, networks, and data processed or stored on any Cobb County computing device. These Security Standards may be updated from time to time by the Information Services Department.

§-II. SCOPE
This policy will apply to all Full-Time, Part-Time, Seasonal, and Temporary Employees; Volunteers, Interns, Vendors, and Contractors to Cobb County. All such people shall herein be referred to as "Users."

§-III. POLICY
County computing devices, software, Internet, and E-mail access are intended to increase productivity of Users in their official duties. All personnel who access or make decisions affecting Cobb County Government's computer based information assets play a role in protecting those assets. Users are expected to use these resources in a manner consistent with County policies, applicable law, and job responsibilities. Users will be held accountable for protecting the County's computer-based information. Inappropriate or illegal use or failure to comply with this or the Information Technology Security Standards may result in disciplinary action up to and including termination.

§-IV. EXPECTATION OF CONDUCT
The County's computing devices and information systems are intended for business use in performing the duties of a User's job. Users should utilize electronic resources in a manner that reflects positively on themselves and Cobb County.

A. Personal Responsibility
Users granted User ID's and access to the County's computing assets are responsible for any and all transactions, inquiries, e-mails, and activities performed with their User ID's. Users shall secure their User ID's to prevent unauthorized use. No User subject to this policy will use the User ID of another User without express permission of the User assigned the User ID.

B. Monitoring
Users are given access to the County's computer network to assist them in performing their jobs. Except for confidentialities created by law (such as attorney-client communications), a User should not have any expectation of privacy in anything created, stored, sent, or received on the County's computer network. Computer files and electronic communications via the Internet or electronic mail are subject to the Open Records Act and the County reserves the express right to monitor, in any way, the activities of a User while engaging in any electronic

communications and to review any material created, stored, sent or received using County computing assets.

C. Sanctions
Violation of this Policy or the Information Technology Security Standards will lead to discipline, which may include restriction or revocation of access, as well as other disciplinary action up to and including termination. Users should also be aware that violation of this Policy or the Security Standards in some circumstances could lead to the imposition of criminal sanctions.

§-V. Policy Standards
The Information Services Policy Standards will address the following areas:

A. Login ID's
Users shall have an Information Services assigned login ID and an associated login password. Login ID's should be cancelled immediately by notifying Information Services in writing when access is no longer required by the User.

B. Passwords
It is the responsibility of the User to protect and secure the County network. Giving passwords to other Users or any other individual for any system or remote access will be subject to the appropriate disciplinary action. The practice of sharing passwords and other User account information may be in violation of Georgia law O.C.G.A. 16-9-90 and is prohibited.

C. E-mail
All messages distributed via the Cobb County E-mail System are the property of Cobb County Government. There **should not be an expectation of privacy** in messages that are created, stored, sent, or received by the County's E-mail System. E-mails may be monitored without prior notification as Cobb County Government deems necessary.

Caution:
Special consideration should be given before communicating confidential and/or sensitive information such as performance reviews, disciplinary and/or correction actions, attorney-client privileged information, personnel information, and health or medical information via electronic communications.

NOTE:
Electronic messages are not recommended as an appropriate form of communication with legal counsel when seeking advice or transmitting information related to litigation or disputes that may result in litigation.

D. Internet
It is the responsibility of the User's Department Head to authorize Internet access and to make sure that the User signs the Internet Access Authorization Form.

Generally Acceptable Uses:
A User who exercises the privilege of using the Internet or e-mail will:

- Use Internet and e-mail technologies to conduct County business.

- Ensure that all communications are professional, truthful, appropriate, and lawful.
- Use language and subject matter that reflects business purposes and is in compliance with County policies and procedures and all state and federal laws.
- Ensure that the activity does not interfere with the User's productivity.
- Be responsible for the content of all communications sent over the Internet. All communications should show the User's name.
- Be responsible for all computer transactions made with the User's User ID and password.
- Verify and ensure the accuracy of any information obtained from Internet resources prior to using such information for a business purpose.
- Engage in limited personal use and only with prior approval of from the User's Department Head or designee. If approved, such personal use shall be incidental, occasional, of short duration, and not result in expense to the County or violate a prohibition under the policy standards, this policy or other County policies.
- Comply with the Cobb County Information Services Department's Information Technology Security Standards.

Generally Prohibited Uses:
Any User who exercises the privilege of using the Internet or e-mail is accountable for his/her actions and communications related to electronic transactions or messages and will not:

- Engage in communicating (creating, sending, copying, or forwarding) any obscene, harassing, threatening, discriminatory, fraudulent, or disruptive messages, e-mail, chain messages, chain e-mail, or any other message or e-mail which violates County policy.
- Access, view or download any non-business related information from any web site, chat room, newsgroup, messaging, e-mail or any other electronic location of an adult nature (obscene, sexual, or pornographic) unless pursuant to County business (i.e. law enforcement).
- Engage in any communication for personal gain, solicit or promote commercial ventures, or engage in other non-job related solicitations.
- Transmit any messages anonymously or using an assumed name; attempt to obscure the origin of a message or misrepresent User's job title or position with the County.
- Engage in any illegal or unethical acts involving electronic communications, including criminal acts outlined in the Georgia Computer Systems Protection Act, O.C.G.A. Sec. 16-9-90, et seq. Criminal acts contained in that statute include: computer theft (unauthorized use with the intention to take, appropriate, obtain, or appropriate the property of another); computer trespass (unauthorized use with the intention of deleting a program or data, of interfering with the use of a program or data, or of altering, damaging, or causing a malfunction of a computer, computer network or computer program); computer invasion of privacy (use with the intention to examine employment, medical, salary, credit, or other financial or personal data without authority); computer forgery (creation, alteration, or deletion of data contained in any computer or computer network); and computer password disclosure (unauthorized disclosure of a password for accessing a computer/computer network).

- Send or forward emails containing libelous, defamatory, offensive, racist, sexist or obscene remarks. If you receive an email of this nature, you should delete it and notify your manager/supervisor, if appropriate.
- Send chain mail.
- Forge or attempt to forge email messages, or disguise or attempt to disguise your identity when sending mail.
- Send Spam messages, viruses, or worms.

E. Dial-in Access
Dial-in access to the countywide network is allowable when remote access is **approved** to perform business duties, job functions, or support activities. Access will be granted via a remote access server. Access must be requested by the User's manager/supervisor and forwarded to the Director of the Information Services Department.

F. Direct Network Access
Users and on-site contractors should use equipment approved by Cobb County Information Services Technical Operations Division to attach to a Cobb County Government network. The Cobb County Information Services Technical Operations Division should be notified immediately of lost or stolen client machines or network interface cards (NIC).

G. Wireless Access
All access points or wireless clients to be installed on the Cobb County network must be approved by the Information Services Technical Operations Division and should be installed by staff of the Information Services Technical Operations Division. The Information Services Technical Operations Division should be notified immediately of lost or stolen client machines or network interface cards (NIC). These devices must be immediately unregistered from all access points.

H. Network Designs/Firewalls
All site network designs must be reviewed and approved by the Cobb County Information Services Technical Operations Division prior to implementation. All site network designs involving external access, such as a vendor, should be reviewed and approved by the Cobb County Information Services Technical Operations Division.

I. Hardware and Software
The physical control and security of hardware and software assets assigned to a department are the responsibility of the Department Head. Computer equipment and computer software must be approved by a designated Cobb County Information Services representative prior to purchase. This includes:

- Desktop computers
- Laptops
- Personal Digital Assistants (PDAs)
- Communications Equipment
- Personal Computing Software
- Non-purchased Software
- Operating Systems
- Application Systems
- Network Devices

J. Vendor Equipment
All vendor supported machines that are attached to the Cobb County data communications network must have Cobb County's anti-virus software loaded. The equipment should be controlled by Cobb County Information Services to ensure the proper anti-virus updates and security patches are installed until the hardware is removed.

K. Disposal of Assets Containing County Data
When computer equipment or storage media containing county data becomes obsolete, all data should be erased from all electronic media before disposal. This erasure should be accomplished by such means as physical destruction or low level media formatting by approved erasure software. The erasure of data classified as restricted should be completed by approved Cobb County Information Services personnel or approved contractors.