Information Technology Security Standards

Effective Date: Adopted 10/05, rev. 3/07, 5/09

1. PURPOSE
Pursuant to the Electronic Communications and Security Policy adopted by the Board of Commissioners on October 25, 2005, the purpose of the Information Technology Security Standards is to provide a clear understanding of expectations and procedures to protect Cobb County Government, its Users, and computer-based information assets. These "Security Standards" apply to all full-time, part-time, and temporary Users of Cobb County government and to all contractors and vendors that access Cobb County's Information Systems, hereinafter referred to as "Users." These Security Standards will be reviewed periodically for technological changes and amended as necessary.

2. SCOPE
The Security Standards apply to Users and to all information processed by or stored on any Cobb County computing device and all County computing platforms unless noted. This document is not intended to be a detailed description of the technology specifications needed to implement a specific project. For detailed specifications, contact the appropriate Information Services Team.

3. EXCEPTIONS
While the business needs of a department may determine the appropriateness of a particular information security standard, exceptions may be justified and approved in advance by the Director of the Information Services Department. Cobb County Government may deviate from this information technology standard when:

- It has been clearly demonstrated that a cost/benefit analysis has been performed showing a) the available compliance options, and b) the risk of noncompliance.
- An acceptable balance between the costs and the risks are acceptable to Information Services.
- Risk acceptance has been formally approved by the Director of Information Services.

4. DEFINITIONS
The following list defines key terms in this document.

- Computing Device - Any electronic device that connects to the County's Network in any way (wired or wireless). Among the partial list of computing devices would be personal computers, laptop computers, personal digital assistants, RIM devices, Blackberry devices, servers, firewalls, switches, routers and hubs.
- Contractor - A person or company who sells labor services to Cobb County Government.
- De-militarized Zone (DMZ) - A network on a firewall that can be accessed from the internal network (the Cobb County Network) and an external Network (Internet). Devices on the DMZ are not allowed access to the internal Network unless special controls are in place.

- Network Devices - Applies exclusively to routers, switches, hubs and bridges (including physically cabled and/or wireless connectivity).
- IDS- Intrusion Detection Server
- Information Assets - Data that is stored on or passes through a Cobb County Computing device.
- Onsite Contractor - A Contractor who performs all daily work at a Cobb County facility.
- Offsite Contractor - A Contractor who performs some or all of the contract work at a non-Cobb County owned facility.
- RAS- Remote Access Server
- User ID - The computer identifier unique to each User granted access to any County computing asset.
- Vendor - A person or company that sells and/or maintains hardware and/or software.
- Voice Applications - Applies exclusively to Private Branch Exchanges (PBX's); Centrex services; IP Telephony systems; voicemail systems; call accounting systems; call center systems; and cellular devices.
- VPN - Virtual Private Network
- IPSec Concentrator - A device in which VPN connections are terminated.

5. INFORMATION OWNERSHIP AND CLASSIFICATION

Information security requirements are based on the value of information in relation to the potential security threats. All computer-based information assets are placed into one of four classifications as determined by Cobb County Government.

Public Information

Public information requires minimal protection. The risk to the government or our customers is negligible if this information is disclosed or modified. This includes information that is required to be public information by law.

Internal Use Only

Internal use only information has unrestricted use within the county; however, because of its personal or business sensitivity, disclosure shall not be outside of Cobb County. Examples include the Exchange Global Address List.

Confidential Information

Confidential information must have one or more of the following attributes:

- Provides information that is protected by law.
- Provides information that is not public record.

Restricted Information

Restricted information is extremely sensitive. Information in this classification must have one or more of the following attributes:

- Outside disclosure is prohibited.
- Outside disclosure would compromise the county's data and network security infrastructure.

6. SECURITY ADMINISTRATION AND AUTHENTICATION

Information security administration is the day-to-day activity that ensures the proper authorization, documentation, and implementation of login IDs and access controls. Because

some system administration access has the potential to influence these security controls, that activity is subject to the standards below.

6.1 User Authentication Standards

User authentication establishes whether a person attempting to use a county information asset is authorized. Currently, authentication is accomplished by the following: A piece of information that the person knows and can enter into the computer system when prompted. For example, a login ID and password (i.e. User name:Doej001234 Password: Indiana543).

Users granted User ID's and access to the County's computing assets are responsible for any and all transactions, inquiries, emails, and activities performed with their User ID's. Users shall secure their User ID's to prevent unauthorized use of their User ID's. No User subject to these standards will use the User ID of another User without express permission of the User assigned the User ID.

6.2 Login ID Standards

All Users are required to read and sign the *Information Technology Security Standards Acknowledgment Form.*

User must have an assigned login ID and associated login password. The standard format for User Login IDs is:

Nnnnn = the first five letters of the User's last name with the first letter in caps.

N = the first initial of the first name of the User. If there is a duplicate name in the system, the middle initial will be used with the letters in caps.

= the digits of your Cobb County ID.

NnnnnN######
Login IDs should be canceled immediately by notifying the appropriate Information Services support staff when no longer required by User.

This standard will be used for all new Users. Existing Users will continue to use their current log-in.

Login IDs may be established for use by non-Cobb County Government Users. Access is granted as needed. A security acknowledgement agreement between Cobb County Government and the User is required for access to internal systems.

When third-party access to Cobb County Government computers or networks is no longer needed, the Cobb County Government Project Manager or the Business Implementation Manager sponsoring the access must immediately notify the Cobb County Information Services Technical Operations Division to remove access.

Login IDs for Cobb County Government and contractual Users will be canceled or suspended if not used for a period of 60 days.

For each User, Login ID's used to identify a User will be the same across all platforms.

Shared Login IDs may be approved by the requesting User's Department Manager and Cobb County Information Services. Shared Login IDs may be established for use by more than one person if the following criteria are met:

- Use of individual Login IDs has a significant negative impact on productivity.
- Conduct of the normal business function requires a workstation be logged on during most working hours.
- Multiple Users with the same access authorizations and job functions use the same workstation(s).
- Users using a Shared Login ID, during a common work-shift, report to the same manager/supervisor during that work-shift.
- Information displayed on the workstation is not confidential or restricted information.
- The manager retains responsibility for the proper use of the Shared Login ID and changes the password at frequent intervals.
- When a Shared Login ID has been authorized to perform an update function, an authorized User must be logged on at all times. Access to the workstation must be restricted physically to authorized personnel or other compensating controls must be established. The manager/supervisor is responsible for enforcing compensating controls.
- Access is restricted to only those applications/information required to perform the required job function.
- Access to internet or e-mail is restricted.

Production IDs that are not associated with a specific User or group of Users may be defined for use by special processes such as network monitoring, batch processing, and operations management. Production IDs must have appropriate compensating controls such as restricted account privileges, non-interactive sign on, no dialup privileges, or locking the ID to a specific workstation implemented to ensure access is limited to the authorized processes.

6.3 Password Standards

Passwords used to authenticate a User Login ID access to county computers and applications, regardless of the classification of the information residing in them, must be stored in a one-way encrypted format so that other Users cannot decipher them.

Passwords used to authenticate Production ID access to the network are:

- A minimum of eight (8) characters long.
- A random mix of alpha (a-z), numeric (0-9), upper/lower case (A/a), and special characters (#, !, %, $, etc.).
- Required to change, at a minimum, once every ninety (90) days. Additionally, shared login passwords shall be changed each time a member of the staff who knows the password leaves the department or employment of Cobb County Government.
- Retained in a history file to prevent people from reusing their most recently used passwords.
- Changeable by the person to whom they belong.

Passwords used to authenticate access to Cobb County Government's computers and applications should not be:

- Easily guessed such as words found in a dictionary, User names, etc.
- Shared with others.
- Reset by anyone other than the appropriate system administration personnel or their designees.
- Written down or otherwise recorded and stored near the access device to which they pertain.
- Displayed in plain text.

Default passwords shall be changed upon first login. Any account password that is not changed from its default within 1 day of account assignment will be disabled. To secure a network, it is the responsibility of everyone to help protect it. Giving out passwords to other Users, vendors, or contractors, for any system or remote access may result in the appropriate disciplinary action. The practice of sharing passwords and account information is in violation of Georgia law O.C.G.A. 16-9-90 and prohibited.

6.4 System Sign-on and Session Management Control Standards

All access to Cobb County Government computers that store Cobb County Government information shall be properly authenticated. Authentication is managed through the use of login IDs and passwords.

Attempts to sign on to the computer with invalid passwords will be monitored. A system log will be maintained to allow timely review and follow-up of all attempts. If there is unusual activity during sign on the offender's manager/supervisor shall be notified by Information Services.

If the number of invalid login attempts exceeds the system specified parameter, the ID shall be suspended until it is reset by an administrator. The information security violation logs of all applications shall be available for review for due cause.

Before leaving the workstation all active software sessions shall be terminated, the User logged off, or the keyboard "locked" to prevent unauthorized access. The workstation shall be configured to lock or suspend a computer session if there is no activity in a predetermined number of minutes. A password shall be required to re-enable the session.

Any login IDs supplied with operating software shall be disabled or renamed and have their password changed immediately upon installation.

Standards must not be created that automate or eliminate the need to enter a password for a User or Shared Login IDs.

6.5 External Access for Dial-in/VPN Internet Connectivity Standards

Dial-in access 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 shall be requested by the User's manager/supervisor.

Telephone lines used for dial-out computer connections shall be configured in the telephone switch (i.e., PBX and Centrex) to refuse incoming calls. **Dial-up modems are not allowed on a network-connected machine with very few exceptions.** The exceptions are "Phone-home" modems connected to large servers/mainframes that have vendor support contracts. These modems will be configured for Dial-out access only. There will not be any inbound dial access on any of these modems. The Dial-out access is for systems with self recognition of problems which automatically report problems to the servicing vendors.

Virtual Private Network (VPN) connections to the Cobb County Network (i.e. cable modem or DSL) must utilize Cobb County Information Services Technical Operations Division supported infrastructures. All Users that have access to the County network from remote locations must have an anti-virus program with current updates. The User's operating system must have all up-to-date patches. Cobb County's approved security software and VPN client shall be installed before access is granted.

Split tunneling shall not be granted in any circumstance.

6.5.1 Virtual Private Network (VPN) Standards

Approved Cobb County Government employees and all authorized third parties (customers, vendors, etc.) may utilize the benefits of VPN's, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Additionally,

1. It is the responsibility of employees and authorized third parties with VPN privileges to ensure that unauthorized users are not allowed access to Cobb County Government internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3. When actively connected to the corporate network, VPN's will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by Cobb County Government network operational groups.

6. All computers connected to Cobb County Government internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers. Below are accepted anti-virus applications:

    - Symantec Anti-Virus

- Microsoft Anti-Virus
- Norton Anti-Virus

7. VPN users will be automatically disconnected from Cobb County Government's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not Cobb County Government-owned equipment must configure the equipment to comply with Cobb County Government's VPN and Network standards.

10. Only the Information Services Department's Security Team-approved VPN clients may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Cobb County Government's network, and as such are subject to the same rules and regulations that apply to Cobb County Government-owned equipment, i.e., their machines must be configured to comply with the County's polices and standards.

12. All authorized third parties shall sign and return the Cobb County Non-Employee VPN Access Request Form

Enforcement
Any employee or authorized third party found to have violated this standard may be subject to disciplinary action, up to and including termination of employment or authorization.

6.6 Direct Network Access Standards

Users and on-site contractors shall use equipment approved by Cobb County Information Services Technical Operations to attach to a Cobb County Government network.

Offsite contractors, vendors and customers must access county network connected hardware and/or software which they support in one or more of the following ways:

- Directly access an application if the application does not allow a connection to:
  - Connect to another machine.
  - Obtain command line access.
  - Perform machine level administrative functions.
- The vendor works onsite with Cobb County Government supervision.

- For VPN network to network connectivity, the organization is required to sign a security awareness agreement that covers potential business losses associated with allowing them to connect to the County network.
- External Users are allowed to use non-Cobb County equipment to access approved Cobb County applications via the Internet.
- Data encryption is required for this type of application.

The Cobb County Information Services Technical Operations Division shall be notified immediately of lost or stolen client machines or network interface cards (NICs).

6.7 Wireless Access Standards

Data transmitted between the client and the access point shall utilize the highest available encryption (no less than 128 bit).

Access points may not accept connections from unregistered client machines. Shared key authentication and client MAC address shall be registered at the access point. Once the device authenticates to the access point, normal system and application authentication will occur.

No access point or wireless client will be installed on the Cobb County network without the expressed permission of the Information Services Technical Operations Division and shall be installed by the Information Services Technical Operations Division staff.

The Cobb County Information Services Technical Operations Division shall be notified immediately of lost or stolen client machines or network interface cards (NICs). These devices shall be immediately unregistered from all access points.

All wireless access shall be authenticated via an Access Control server or a centralized Authentication server. The Authentication Server will be configured and/or monitored by the Information Services Technical Operations Division.

Installation of a device in a non-approved manner may result in disciplinary action.

7. Physical Access Controls

Access control includes physical access to information processing equipment and data. Physical access controls help ensure that all computing equipment is properly safeguarded and available for its intended purpose.

7.1 Physical / Environmental Controls Standards

Application servers, file and print servers, and telecommunications equipment shall be located in rooms that meet the following physical control standards:

Existing Facilities

- Each room must have a designated owner responsible for authorizing and periodically reviewing who has access to the room.
- Physical access shall be restricted to personnel with a business need to be in the room.

- Keys/combinations shall be distributed to authorized personnel only.
- Combination locks shall be changed from the manufacturer defaults as soon as possible after installation and shall be changed periodically after that.
- Rooms shall not be used for unrelated purposes such as storage of janitorial supplies, office supplies, etc.
- An uninterruptible power supply (UPS) shall be installed to ensure a constant and steady supply of electricity.

New Facilities

- Each room must have a designated owner responsible for authorizing and periodically reviewing who has access to the room.
- Physical access shall be restricted to personnel with a business need to be in the room.
- Keys/combinations shall be distributed to authorized personnel only.
- Combination locks shall be changed from the manufacturer defaults as soon as possible after installation and shall be changed periodically after that.
- Rooms must not be used for unrelated purposes such as storage of janitorial supplies, office supplies, etc.
- Rooms shall be equipped with appropriate environmental controls to maintain temperature and humidity levels that are within manufacturer specifications.
- Rooms should be equipped with fire detection/extinguishing equipment.
- An uninterruptible power supply (UPS) shall be installed to ensure a constant and steady supply of electricity.

7.2 Storage Media Standards

All storage media shall be labeled for easy identification.

All data storage media shall be stored in compliance with the manufacturers' instructions.

All boot tapes / boot CD-ROMs shall be controlled. Elements of control must include precise inventory records, secure physical storage, and strict authorization for usage.

7.3 Disposal of Assets Containing County Data Standards

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

8. Access Standards

Access Standards help ensure that all computer-based information is processed in accordance with proper management authorization.

8.1 Protocol Analyzers Standards

Protocol Analyzers (network monitoring devices, scanning and intrusion/detection software, or "sniffers") will be used for network and server support by Cobb County Information Services Technical Operations Division. **A User found using these**

tools without proper authorization is subject to disciplinary action up to, and including, termination of employment.

8.2 Remote Control Access Standards

Remote control software allows an authorized Information Services support person to take control of another network-connected PC. Remote control access is allowable when remote control is needed to perform business duties, job functions, or support activities. Remote control must not be used to access Cobb County computers without notification to the User using the computer to be controlled by a remote session.

Prior to connecting to a User's machine, each authorized support person using remote control access must identify himself or herself to the User (provide User ID and manager/supervisor name if necessary), identify the reason why he or she wants to take remote control of the User's PC, and identify what he or she intends to do. The User shall be asked to give verbal approval for the remote control access prior to connecting.

Passwords must remain confidential during the remote help session. The authorized support person using remote control must request that the User enter all IDs and passwords when necessary.

9. Internet / Intranet Standards

The Internet is the worldwide collection of networks that are external to Cobb County Government. The Intranet is the collection of Web servers within Cobb County Government. It is the responsibility of the User's department head to request authorization of Internet access from the Director of the Information Services Department and to confirm the User signs the Internet Access Authorization Form.

All persons requesting Internet access must sign an Internet Access Authorization Form that includes acceptable usage guidelines. The Cobb Web Intranet page provides a link to this form.

Cobb County Government confidential information shall be protected by User level identification and authentication if it is available on a Web page.

Cobb County Government Restricted information should not be transmitted over the Internet.

All access points between Cobb County Government networks and the Internet shall be through access points managed by Cobb County Information Services Technical Operations Division.

9.1 Internet Web Site Standards

All county domain names shall be approved by the County Attorney's Office and the domain name registration controlled and maintained by the Cobb County Webmaster.

Content shall be approved, prior to publication, by the owner and the Cobb County Webmaster.

A copyright statement must appear at the bottom of each page.

A Privacy Policy statement shall be displayed on any site that collects information.

9.1.1 Internet 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.
- Show User's name on all communications.
- 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.

9.1.2 Internet 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.
- Engage in the use of streaming audio or video without the approval of the User's Department Head and the Director of the Information Services Department.

9.1.3 E-mail System Standards

- All messages distributed via the Cobb County E-mail System are the property of Cobb County Government.
- No employee should expect privacy in messages created, stored, distributed or received via the Cobb County E-mail System.
- Each employee will ensure that all E-mail communication is professional, truthful, appropriate, and lawful.
- Each employee is responsible for the content of their communications sent from the Cobb County E-mail System.
- Each employee must show their user name on all E-mail communications.
- General standard for an E-mail message retention:
    - E-mail that is not deleted from the Inbox folder, Sent Items folder or any folder established on the E-mail account or archived by the customer is retained, and there is no automatic deletion.
    - E-mail deleted from the Inbox folder, Sent Items or any folder established on the E-mail account is sent to the Deleted Items folder.
    - E-mail that is deleted by the customer from the Deleted Items folders is available for retrieval from our backup system for 14 days after the date it was deleted from the deleted items folder.
    - E-mail not deleted from the Deleted Items folder is retained, and there is no automatic deletion.
- Archived E-mail standard for an E-mail message retention:
    - E-mail that is sent to E-mail folders in an Archive Directory located on the C: drive of the individual's personal computer is not backed up and is not administered by I.S.; therefore, the retention will be dependent on the individual.
    - E-mail that is sent to E-mail folders in an Archive Directory located on the G: drive will be backed up and the back up will be administered by I.S.
- The retention rules for the E-mail archive located on the G: drive is the same as the General procedures for an E-mail account.

9.2 Intranet Web Site Standards

Information published on an intranet web site must have, at minimum, the following information:

- Contact name
- Document retention information

10. Network Designs/Firewall Standards

All site network designs shall 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, shall be reviewed and approved by the Technical Operations Division.

All firewalls used for external access must be owned by the Cobb County Government and installed by the Cobb County Information Services Technical Operations.

There shall not be full open access from the outside to the inside of the county network.

11. Network Standards

Notification of all network devices shall be given to Cobb County Information Services Technical Operations Division for testing and approval.

All site network designs shall be reviewed and approved by the Cobb County Information Services Technical Operations Division prior to purchase.

Standards as defined by the Cobb County Information Services Technical Operations Division shall be followed for all:

- IP address ranges
- Subnet masks
- Network device names
- Protocols

Administrative access to all network devices shall require an ID and password. Please refer to the password section for the standard convention.

12. Voice Standards

Notification of all voice applications shall be given to Cobb County Information Services Technical Operations Division for testing.

Cobb County Information Services shall be notified when changing standard configurations for testing:

- System configuration and design
- Network configuration and design
- Telephones or soft phones

13. Hardware and Software Standards

It is the policy of Cobb County Government to centrally control expenditures for computer equipment and software and require review and approval from Cobb County Information Services before authorization of such expenditures. Computer equipment and computer software shall be approved by a designated Cobb County Information Services representative prior to authorization. This includes:

- Desktop Computers
- Servers
- Laptops
- Personal Digital Assistants (PDAs)
- Communications Equipment
- Personal Computing Software
- Non-County purchased Software
- Operating Systems
- Application Systems

The software that comprises the County Desktop image shall be installed on all Personal Computers in the County with the following exceptions:

- Variations of the Desktop may be implemented with approval from the Cobb County Information Services Client Services Manager with notification to the Cobb County Information Services Technical Operations Division.
- PCs used for specialized functions such as laboratory analysis or Production line control are exempt.
- Other PCs, with sufficient business justification, are exempt from using the standard desktop image.

The physical control and security of hardware and software assets is the responsibility of each Cobb County Government business unit department head.

The following activities are **PROHIBITED:**

- Storing, installing, maintaining, or keeping any personal files, such as photos, music or videos, on County supplied computing devices without approval the employee's Department Head and the Director of the Information Services Department.
- The installation of non-approved or User-owned software including freeware, shareware, or drivers on county PCs.
- The installation of Cobb County-owned software on User-owned PCs, unless approved by the Information Services Department.
- The use of file sharing programs including, but not limited, to Kazaa, Napster, LimeWire, or Morpheus.
- The installation of any non-approved hardware onto the County Network or into a County-owned computing device.

The Information Services Department may run scanning tools and any other software available to control the use and to protect the network. Any User who runs unauthorized software will be in violation of these standards which may result in disciplinary action.

The use of port scanners, password cracking tools, or any hacking, information gathering, or other harmful software deemed such by the Information Services Technical Operations

Division on the Cobb County Intranet is prohibited without prior approval of the Director of the Information Services Department.

Users must take special care to protect their assigned equipment from theft or loss. Any laptop, handheld or portable network device will not be allowed to store the passwords on the client. Any stolen portable device shall be reported immediately to Risk Management and the Information Services Technical Operations Division.

All portable devices shall be approved prior to installation to make sure that they are up-to-date with the appropriate controls software.

13.1 Standard for Employee Owned Personal Digital Assistants (PDA's)

It is against policy to attach non-County owned computing devices to the County Network. However, there are instances when an employee owned Personal Digital Assistant (PDA) can improve the employee's productivity by synchronizing the employee's appointment calendar and e-mail maintained on the County's Outlook/Exchange System to their personally owned PDA.

Therefore, this standard is in support of improving employee productivity by using a personally owned PDA to synchronize with the County's Outlook/Exchange Servers.

- Any personally owned PDA device must be Blackberry or Goodlink or Windows Mobile Messenger compliant, if a personal PDA device is not compliant with one of these three (3) standards it may not synchronize with the County's Outlook/Exchange System,
- Before attaching to the County's E-mail System the employee must obtain the written approval of their department head and the Information Services Director,
- The Technical Operations Division of the Information Services Department must be notified before the device is synchronized with the County's Outlook/Exchange System,
- The device must be password protected,
- The device and all required licenses must be acquired, paid for and maintained by the employee,
- No cost, initial, or otherwise will be paid by the County.

The County's Technical Operation or Client Services Divisions will assist with the setup of the device.

The Technical Operations and Client Services Divisions will provide assistance to the device owner for problem diagnosis and resolution when possible; but is not responsible for the support, maintenance or operation of the device.

If a personally owned device is lost or stolen the Technical Operations Division of Information Services must be notified as soon as possible.

14. IP Addressing Standards

IP addresses will **ONLY** be given out by a member of the Information Services Technical Operations Division. Once an IP address is assigned the appropriate MAC address and location of the equipment shall be forwarded to a member of the Information Services Technical Operations Division within 24 hours. When equipment connected to the Cobb County data communications network is moved, the Cobb County Information Services Technical Operations Division shall be notified within 24 hours.

If this procedure is not followed, the Cobb County Information Services Technical Operations Division shall notify the User's manager for appropriate disciplinary action.

15. Vendor Equipment Standards

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 shall be controlled by Cobb County Information Services to ensure the proper anti-virus updates and security patches are installed until the hardware is removed.

16. Asset/Privileged Access Standards

When a User is issued equipment, keys, remote access, portable computers, diagnostic equipment, tools, or anything purchased by Cobb County Government, a departmental tracking form shall be completed and will be maintained in the User's department maintained personnel file. This is to ensure the proper recovery and termination of access to systems.

The Human Resources Department and terminating manager must gather all Cobb County keys that were assigned to the User. All badges will be collected and the Sheriff's Office or Police Department, or any Department responsible for programming security access badges, will be notified. All county property such as beepers, cell phones, laptops, handhelds or any other tools/devices assigned to a User shall be returned to the managers of the department from which the User is terminated.

Information Services shall be notified immediately via e-mail of terminations so User accounts and remote access can be disabled.