INFORMATION TECHNOLOGY AND HIPAA POLICY

Section 1: Purpose

The purpose of this policy is to help provide a safe and secure network for users as well as to ensure that the use of technology resources is consistent with all Chatham County policies, all applicable laws and individual job responsibilities. This policy is not meant to contradict Chatham County's established culture of openness, trust and integrity. This policy applies to any user of Chatham County's technology resources and applies at all times and all places, regardless of if the user is on or off the job. Chatham County is referred to as "County" throughout this policy.

County technology resources include equipment and systems that are owned, leased, used, managed or operated by the County. Technology resources include, but are not limited to:

- All computer hardware such as keyboards, docking stations, mice, and monitors
- Scanners and desktop printers
- Desk phones, smart phones and cellular phones
- Fax machines
- Voicemail systems
- Electronic messaging systems
- Software
- Audio/video equipment (TV's, projectors and speakers)
- Network resources (i.e. "S" and "H" drives)
- Internet resources
- Digital cameras
- Flash drives
- Portable hard drives
- Key fobs and access cards
- GPS devices
- SD cards
- Tablets

All technology resources are the property of the County and are made available to help employees and officials provide services in a timely, efficient and effective manner. Any activity, use, or action that is inconsistent with this policy is prohibited. Because technology resources are constantly evolving, the County requires all officials and employees to use their best judgment in complying with the rules set forth in this policy. The content herein applies to all County technology resources which include hardware, software, and digital, regardless of physical location or time of day.

This policy is intended to illustrate the range of acceptable, unacceptable, and prohibited uses of the County's technology resources and is not exhaustive. It also serves as notice to users that there is no expectation of personal privacy in the use of County technology resources.

This policy may not be waived or modified by any employee, except as set forth in policy.

Section 2: Definitions

***Bandwidth*:** The rate and volume of data transferred.

***Electronic Messaging*:** The electronic distribution of messages, documents, files, software or images (including e-mail, text messages, tweets, voice mail messages, Skype, etc.).

***E-mail*:** The electronic distribution of messages, documents, files, software or images over a phone line or network connection. This includes internal e-mail and external e-mail to personal accounts (such as Yahoo, Hotmail, etc.).

***"H" Network Drive*:** Each County official and employee is provided with the network drive designated as the "H" drive, which serves as storage space for their files. These drives are backed up nightly.

***Internet and the World Wide Web*:** A system of Internet servers that support documents specially formatted in HTML (*Hypertext Markup Language*).

***Intranet*:** A private network for communications and the sharing of information that is accessible only to County officials, County employees and others who are on the County's network.

***Local Drive*:** All County computers have one local drive. It is used for the storing of programs or data. Employees should create and edit their "original" documents on the local drive and only a copy should be shared and stored on any network shared drives.

MIS (Management Information System): The Department in Chatham County that is responsible for managing technology resources.

***Network*:** A system by which many computers are connected together. Chatham County's network gives users access to authorized areas on the different computer systems. This includes access to printers and the department's shared drives.

***Outside Data Source*:** Any file, program, image (pictures) or document received on media (CD's, flash drives, etc.) through the Internet or through file transfer.

***PC*:** Personal computer (i.e. workstation, desktop, laptop, notebook, etc.)

***Phishing*:** Act of tricking users into revealing account information, such as usernames and passwords, by sending them e-mails from a false source, calling to request information or asking for information in person.

***Post*:** A comment made to a social networking page or other interactive site. For example, Facebook users can post to another user's "wall" or Intranet users can post a comment on an existing blog.

***Shared Drives*:** These drives are to be used to store information that needs to be shared on a regular basis between employees within a department.

***Social Networking*:** Use of a variety of web sites that allow users to share content, interact and develop communities around similar interests.

***Spam*:** Unauthorized and/or unsolicited electronic mass mailings.

Spyware: Software that send information about your Web surfing habits to its Web site.

***User*:** County officials, County employees including those who are temporary, part-time, vendors or contractors and any other person with access to County computers.

***Virus*:** A program or script that can infect other programs by modifying them in a malicious way usually resulting in the corruption of a system and/or the slowing of its operations dramatically. For the purpose of this document, spyware can be considered a form of virus.

VPN (Virtual Private Network): A connection set-up on a device that allows employees to work from home and have access to the County network.

***Web Server*:** A computer or virtual device that delivers (serves up) web pages

Section 3: Information Access and Ownership

All technology resources and all information created, received, sent and stored on County systems are the property of the County. The County reserves the right to monitor the information without notice to the employee. This information includes, but is not limited to:

A. Voicemail

B. E-mail and any other media (videos, pictures, files). Access and monitoring might be undertaken for a number of reasons. For further clarification on what may be grounds for the County to access and/or monitor an official or employee's system, contact Human Resources.

If a department head needs access to an employee's information, he or she must enter a help desk request requesting access. The MIS Director will then contact the Human Resources Director, or designee, via the request asking that permission be granted to the department head. At times, it may only be appropriate for Human Resources to access the information. Although MIS staff has access to all employee information, they will not monitor employee accounts or information unless Human Resources or the MIS Director has asked them to do so. Officials and employees shall have no expectation of privacy or confidentiality when using the County's technology resources, even if the technology resource is protected with user ID or password.

Section 4: Public Records

Documents created, stored, sent and/or received using the County's computer network may constitute public records. Any public record may be inspected and/or copied by any person for any reason. Public records include, but are not limited to:

A. Email messages (includes employee personal email accounts if checked from County computers or cell phones)

B. Text messages

C. Telephone records

D. Content posted on social media sites

E. Any other electronic message created, received, sent and/or stored by the County

For detailed information on public records law, refer to the Chatham County's Public Records Policy.

Section 5: Electronic Messaging, Internet Usage, and Social Media

Electronic messaging includes, but is not limited to email, instant messages, text messages, blog posts, forum posts, wiki posts, social media site posts, images and audio or video recordings. Electronic messaging may not be used in any way which violates the County Social Media Policy (located on the internal web).

A. County employees shall identify themselves clearly and accurately via e-mail and the Internet. Anonymous or pseudonymous posting is expressly forbidden.

B. All employees must sign and abide by the County Social Media policy.

C. Personal use of external interactive chat sessions is prohibited (i.e. GTalk, Yahoo, etc.)

D. The use of personal e-mail accounts for County business is prohibited. (For example: Hotmail, Yahoo Mail, Gmail, etc.). Internet e-mail (Pop, IMAP or Web based e-mail) circumvents security measures and is strictly prohibited.

E. Personal use of a County email address for non-business functions such as Ebay, Facebook, Twitter, Craigslist, etc. is prohibited.

F. It is strongly recommended that officials and employees use a disclaimer in their outgoing e-mails as a reminder to the receiver that electronic correspondence is public record.

G. Officials and employees should not open e-mail and/or attachments sent from an unknown sender as these may contain viruses that can infect their computers.

H. Information Technology will only support approved Web browsers.

I. Any software or files downloaded via the Internet into the County's network become the property of the County. Employees with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered. Software licensed for free personal use cannot be used for business without being purchased and licensed.

J. Employees should be aware that trial software is good only for the trial period and must not be re-installed for additional trial periods without the purchase of said software. These installs will only be done by MIS with employee department head approval.

K. Downloading software, files, screensavers, pictures, and images uses network resources, memory and/or disk space and may corrupt your PC. Downloads shall have a direct business- related use.

L. County employees are expected to use the Internet and information processing resources responsibly and professionally at all times. County employees may make reasonable

personal use of County owned or provided Internet resources, with department head approval, as long as:

1. the direct measurable cost to the County or its citizens is none or is negligible
2. there is no negative impact on employee performance of duties
3. personal use is conducted on an employee's own time
4. use does not interfere with other employees performing their jobs or undermine the use of County resources for official purposes
5. employees reimburse the County if costs are incurred
6. use does not violate applicable laws or regulations
7. use does not violate County policies

M. Personal use of streaming audio/video from such sites such as YouTube, news sites, web conferencing, or radio stations is prohibited. If the use of these resources is needed for work related reasons, it must be approved by the employee's department head and MIS.

N. Links from the County website to other Web sites will be at the discretion of Chatham County.

O. Employees are expressly prohibited from visiting inappropriate or sexually explicit sites unless required for investigative purposes in the performance of their job.

P. Employees are expressly prohibited from storing inappropriate, obscene or sexually explicit material on any County owned equipment or storage device unless required for investigative purposes in the performance of their job.

Q. Employees with Internet access may not use County Internet facilities to download entertainment software or games, or play games against opponents over the Internet. Employees may not use County Internet services to request that images or videos be downloaded unless there is an explicit business related use for the material.

R. No employee may utilize the County's network or resources to establish, construct, design, update or publish a personal web site. No employee shall alter, amend, or edit any existing County web site without permission from the Department Head or MIS.

S. No County equipment will host a service (application, web, email, program, etc.) of any kind unless approved by the employee's department head and MIS.

T. Personal use of County resources by an employee neither expresses nor implies sponsorship or endorsement by the County.

U. Use of the County's technology resources for operating a personal business or soliciting of any kind is prohibited.

V. Personal use of peer to peer file sharing and cloud storage is prohibited due to the significant security threat posed. These services include but are not limited to DropBox, Google Drive, Skydrive, torrents, etc.

W. No employee should have any expectation of privacy as to his or her Internet usage or electronic messages while using a County owned computer or mobile device; all can be monitored and periodically audited at the request of Human Resources.

X. County resources shall not be used to violate State or Federal copyrighted materials law. Not all material that appears on the world wide web is free to use. Electronic documents, images, and videos are considered copyrighted at the time of their creation without. Filing a copyright application is not required.

Section 6: Hardware Use

Any hardware provided by the County is strictly to be used solely in the fulfillment of job responsibilities. Use of any County property for personal gain whether for financial profit or other compensation is prohibited. Employees must adhere to the following:

Computers and Peripherals

A. County computers and peripherals (i.e. mice, keyboards, speakers, etc.) are for conducting County business. Personal use of these devices during lunch breaks must be approved by the employee's department head.

B. Employees may not connect **personal** devices on County computers as these can pose a threat to the network security. These devices include, but are not limited to:
    1. Flash Drives
    2. Audio media players (iPod, MP3, MP4, etc.)
    3. Cameras
    4. SD Cards
    5. External hard drives
    6. Tablets or iPads
    7. CD's or DVD's (audio or software)
    8. Personal cellular phones

Printers, Copiers, and Fax Machines

C. Photocopy machines, printers and fax machines shall be used for the transaction of County business. Any personal use must be pre-approved by the Department Head and reimbursement for personal use should be arranged with the Department Head prior to use.

D. Unauthorized copying of copyrighted material is strictly prohibited.

Cell Phones and Desk Phones

E. Personal use of desk phones and cell phones must be kept to a minimum and must result in NO COST to the County. Calls that result in charges to the County must be reimbursed at the current per minute rate plus any other applicable fees that may apply. The department head will talk with the employee if charges are incurred and make arrangements with him/her for reimbursement.

F. Personal incoming calls should be discouraged.

G. Downloading apps on smartphones is discouraged. Should an employee incur charges for the purchase of apps (not related to job responsibilities), s/he will make arrangements with the department head for reimbursement.

H. Employees who have been authorized by their department head to access email on a personal phone must allow access, either through firmware or software, for MIS to delete all County data on that phone in the event of a loss, theft, or if the employee no longer works for the County.

County-owned equipment assigned to an official or employee is his or her responsibility. Should equipment be damaged or stolen, the official or employee must report it to his or her department head and to MIS immediately.

Section 7: Security

The MIS department will deploy and maintain all security measures for all County information technology resources. Employees and officials are required to follow the security steps listed below.

User ID's and Passwords/ PC Security

A. All County officials and employees will have a user ID and password to access County e-mail and log into their computers. Some users may have multiple user ID's and passwords depending on access to other systems, such as the AS-400. User IDs and passwords are set-

up to protect the County's technology resources and not to give employees any expectation of privacy in records or information protected by user IDs and passwords.

B. **Log-ins and passwords should never be shared with others**. Working under someone else's user ID and password is prohibited. Anyone using the County's technology resources is responsible for all actions taken while using their personal user ID and password.

C. Passwords are set to force officials and employees to change them every 90 days. Officials and employees cannot repeat the previous twenty-four passwords used. Passwords must contain at least 8 characters, which include a combination of letters, numbers, and special characters such as !, #, $). Employees should **not** write their passwords down, post them anywhere or store them within a file on their computer. If an employee changes his or her password and forgets it, he or she must ask a co-worker to submit a request through help desk to have it reset. The request must include a phone number where the user can be reached to receive the new password.

D. Department heads or their approved designees must request a user ID and password for new employees prior to their first day of work by submitting a request through help desk. When a user is no longer a County employee, Human Resources will follow the Exit Process Procedures to ensure that access to the network be shut off and other technology resources be returned. In cases of an emergency, the County Manager's Office may inform MIS through alternative means as deemed necessary.

E. Officials and employees must not leave PCs unattended without first logging off or locking the PC. This can be done by pressing CTRL + ALT + DELETE and clicking on "LOCK THIS COMPUTER." Officials and employees are required to log off their computers at the end of the work day. If an employee leaves a computer unattended and unlocked, any actions taken by others on that computer that violate policy or the law will be the responsibility of the employee who is logged in. Activity on any County device is associated with the employee username and password.

Other

F. All PC's shall have approved anti-virus software installed and functioning at all times.

G. Only MIS employees will have full administrator privileges on servers, desktops, or other devices.

H. Virtual Private Network (VPN) is the County's preferred method of connecting to its network while out of the office. Only authorized employees are allowed VPN access. Use of

this service requires software that is installed by MIS on County owned equipment only. VPN access must be approved by the employee' department head and MIS.

I. Remote access for third parties (vendors, customers, etc.) will be requested by the department head via a request through help desk.

Section 8: Confidential Information

A. Any information sent through electronic means is at risk for being interrupted or compromised by hackers. Officials and employees should not send confidential information (i.e. medical records, client information, etc.) electronically. If an official or employee is uncertain about sending a particular piece of information electronically, he or she should check with his or her department head before sending.

B. When an employee is uncertain whether or not information is confidential, the employee should err on the side of caution and obtain approval before transmitting

Section 9: Other Activities

A. Employees using the County's technology resources are representing the County. Employees are expected to use these resources responsibly and professionally.

B. Examination, modification, deletion, or copying of data belonging to other employees without their consent is prohibited, with the exception of the MIS employees while acting in their official capacity.

C. When there is an implementation of new software in a department, it is the responsibility of the department head to ensure that employees are adequately trained on how to use it.

D. MIS will authorize the purchase of hardware and software for the County (see page 3 of the Purchasing and Contracting Policy). MIS will not be responsible for supporting items that were not approved for purchase.

E. It shall be the responsibility of the department heads to ensure that their employees have read and fully understand this policy. If employees have any questions, they should contact their department head or MIS.

F. If an employee uses technology resources in a manner that violates this policy or other County policy, the County will take appropriate disciplinary action up to and including

dismissal. Furthermore, the County will cooperate fully with any legitimate law enforcement investigation and subsequent prosecution relating to an employee's violation of this policy

Approved by:

_____ _____

Charlie Horne, County Manager Date