Process: Information Security and Accountability Policies Handbook
Document#: 500-010
Original Author: Matthew H. Ury, Director of Information Technology
Last Updated: 1/6/2021
Approved by: Wayne County Board of Supervisors
Resolution: 551-20
Date: 12/15/2020

Revision History			
Revision Date	#	Initials	Summary of changes
09/22/2020	1.0		Initial Review
11/19/2020		AP	Grammar checked
1/6/2020	2.0	MU	Resolution and date added

Introduction

Technology is constantly evolving. Policies and procedures should be amended in response to the ever-changing technological environment. Exceptions “to the rule” should be an extremely rare occurrence and only sanctioned as temporary responses to urgent situations. Security should not be compromised for expediency.

Confidentiality Notice

This document is intended for the internal reference of Wayne County employees **only**. External reproduction and/or distribution of the material contained herein is strictly prohibited without the expressed permission of the Wayne County IT Director. The most up-to-date copy of this document is available under County Polices on the Wayne County Internal Website http://insideweb/

Information Security and Accountability policies will be reviewed annually, and updated as needed by the IT Director and Compliance Officer.

Information Security and Accountability

Preface

The Wayne County IT Information Security and Accountability policies are a statement of the minimal requirements, ethics, responsibilities, and accepted behaviors required to establish and maintain a secure environment. Further, these policies facilitate the County’s acceptable use and information security objectives. Compliance with these policies, guidelines, and procedures is expected and it is the responsibility of each Wayne County department to ensure their individual compliance.

Purposes

The purpose of this document is to ensure the confidentiality, integrity, and availability of computing resources by defining a set of minimum policies, guidelines, and, procedures. These minimal definitions outline the appropriate use, acquisition, and implementation that all Wayne County departments should strive to meet. This documentation applies to all Information Technology hardware, software, facilities, applications, and networks that are collectively referred to as Wayne County’s computing resources. This documentation shall also serve as best practices for the County of Wayne; inclusive of all campus locations. Any department may, based on individual business needs and specific legal requirements, exceed the guidelines put forth in this document, but should, at a minimum, achieve the security levels outlined herein. Such additional requirements, such as the Health Insurance Portability and Accountability Act (HIPPA), USDOT Pipeline, and Hazardous Materials Safety Administration, are examples of such external requirements.

All users have the responsibility to maintain, and protect Wayne County’s information assets against accidental or intentional disclosure, compromise, and/or loss. Each user also bears the responsibility of maintaining and protecting the County’s public image. It should be the intent of every employee utilizing Wayne County’s information systems to do so in a manner that reflects productivity, integrity, and appropriate transparency.

The primary objectives of the Information Security policy are as follows:

- Communicate the responsibilities for the protection of County information and provide guidelines for County employees in relation to the acceptable use of Wayne County-owned resources. These resources include, but are not limited to: personal computers, copy equipment, printers, cell phones, air cards, office phones, wired and wireless networks.

- Provide guidelines for Wayne County departments to effectively manage their IT related assets, as well as the management of security exposure/compromise risks within County systems.

- Preserve management's options in the event of an information asset misuse, loss, or unauthorized disclosure of information.

Scope

These policies and procedures apply to all County departments, but are not intended to unilaterally change the terms and conditions of employment. All County departments, when coming into compliance with these policies, guidelines, and procedures, should consider all terms and conditions of employment, as well as collective bargaining agreements.

These policies, guidelines, and procedures are applicable to all County departments, staff, and all others which include all outsourced third parties which have access to or manage County information. Where conflicts exist between these policies, guidelines, and procedures, and a County department guideline, the more restrictive guideline should take precedence.

These Wayne County IT Security and Confidentiality Policies encompasses all systems; automated or manual, for which the County has administrative responsibility, including systems managed or hosted by third parties on behalf of the County. It addresses all information, regardless of the form or format (including, but not limited to electronic, paper, and voice), which is created or used in support of business activates of County departments. Throughout these documents, all references to protected information should be interpreted as inclusive of all types of sensitive information, whether or not that is explicitly mentioned. This includes, but is not limited to: Personal or private information (PPI), Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII), financial information, AND electronic and hardcopy protected or private information. These policies and procedures should be communicated to all staff and all others (with signature) who have access to or manage County information. This document is posted on the Wayne County intranet for reference.

Security and Accountability Overview

All information, regardless of the form or format, which is created, acquired, or used in support of Wayne County business activities, should only be used for County business. County information is an asset and should be protected from its creation, through its useful life, and to its authorized disposal. It should be maintained in a secure, accurate, and reliable manner and

be readily available for authorized use. Information should be classified and protected based on its importance to business activities, risks and security best practices.

Information is among Wayne County's most valuable assets and County departments rely upon that information to support their business activities. The quality and availability of that information is essential to the department's ability to carry out their missions. Therefore, the security of the County's information, and of the technologies and systems that support this, is the responsibility of everyone concerned. Each authorized user of the County's information has an obligation to protect this information in a consistent and reliable manner. Security controls provide the necessary physical, logical, and procedural safeguards to accomplish those goals.

Information security management enables information to be shared, while ensuring protection of that information and its associated information technology equipment including the network over which the information travels. County designated staff are responsible for ensuring that appropriate physical, logical, and procedural controls are in place on these assets to preserve the security properties of confidentiality, integrity, availability, and privacy of Wayne County information.

Individual Accountability

Individual accountability is the cornerstone of any security program. Without it, there can be no security.

- Access to County information technology equipment, systems, and networks where the Department Head (Information Owner) has identified the business need for limited user access or information integrity and accountability should be provided through the use of individually assigned, unique identifiers known as Network IDs, or other technologies including biometrics, token cards, etc.

- Individuals who use County information technology equipment should only access information assets to which they are authorized and for which they have a specific job-related need.

- Individuals are not to download and Protected Health Information or any other protected or sensitive information (as described on page 5 of this document) except as needed for their assigned job duties.

- Associated with each Network ID is an authentication token such as a password which should be used to authenticate the person accessing the data, system, or network. Information used to authenticate the identity of a person or process should be treated as confidential and should not be disclosed. This does not include distribution of one-time-use PINs, passwords, or passphrases.

- Each individual is responsible to reasonably protect against unauthorized activities performed under their Network ID. This incudes, but is not limited to the locking of computer screens when leaving them unattended.

- For the user's protection, and for the protection of County resources, Network IDs and passwords (or other tokens or mechanisms used to uniquely identify an individual) **should not be shared.** This information should not be visibly posted or written down unless in a password protected document.

Confidentiality, Integrity, and Availability

- All County information should be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. The information owner should classify and secure information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.

- Appropriate processes will be identified in the Wayne County Continuity of Service Plan to ensure the reasonable and timely recovery of critical County information, applications, systems, and security regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period.

Policy Monitoring and Enforcement

Computer systems and resources provided by Wayne County are owned by the County and are therefore its property. This gives Wayne County the right to monitor any and all voice and data traffic passing through its system. (This includes, but is not limited to e-mail, voice messages, internet use, and history.) Back-up copies of voice and data traffic may exist, despite user deletion, in compliance with Wayne County's records retention policy. The goal of these back-up and archiving procedures are to ensure system reliability and prevent business data loss.

Caution should be used when communicating confidential or sensitive information via e-mail. All e-mail messages sent outside of Wayne County become property of the receiver. In addition, all e-mail records that concern County business are subject to FOIL (Freedom of Information) requests from the public.

Reporting Misuse

Any allegations of misuse should be promptly reported to the head of the department and also to the Director of Information Technology at 315-946-7450. Offensive or suspicious e-mails should not be forwarded, deleted, or replied to. Instead, a report should be made directly to the individuals named above.

Disclaimer

Wayne County assumes no liability for the direct and/or indirect damages arising from an employee's use of Wayne County's voice or data services. Employees are solely responsible for the content they disseminate. Wayne County is not responsible for any third-party claim, demand, or damage arising out of the use of the County's voice or data services.

Failure to Comply

Violations of any Information Security Policy will be treated like other allegations of wrongdoing at Wayne County. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of County voice or data services may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of access to voice or data resource.
- Disciplinary action according to applicable County policies
- Termination of employment.
- Legal Action according to applicable laws and contractual agreements.

Organizational Security and Functional Responsibilities

County Departments

Each County department should have a process in place for determining information sensitivity, based on best practices, State and County directives, and legal and regulatory requirements to determine the appropriate levels of protection and access by users for that information. The head of each County department should ensure that an organization structure is in place for:

- The implementation of acceptable use practices and information security guidelines and procedures.

- The implementation of an internal security awareness program.

- Monitoring significant changes in legal or regulatory requirements and in the exposure of information assets to threats.

- Responding to security incidents.

- Communicating requirements and procedures to all departmental users (employees and third-parties) and including these in third-party agreements and contracts. These expectations should be reviewed annually with users, and it should be verified that they signed an Employee Information Security Policy Agreement; signifying that they have read, understand, and agree to their responsibilities as listed in the Wayne County IT Security and Accountability Policies, and that they have been trained on the handling of all sensitive and PHI data.

- Reviewing these established procedures and internal audits with the Information Technology Department and Compliance Officer annually.

Information Owners

Wayne County departments are considered the information owners for the data and tools they administer. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be. These access privileges should be in accordance with the user's job responsibilities. Information owners also communicate, to the Director of Information Technology, the legal requirements for access and disclosure of their data. Individual departments are responsible for the maintenance of appropriate security measures such as assigning and verifying information asset classification and controls, managing user access to their resources, communicating deficiencies in controls to the Director of Information Technology and/or the County Administrator. Responsibility for implementing security measures may be delegated, though the accountability remains with the identified owner of the asset. Each department which handles any type of protected information (as described on page 5 of this document) should have a defined system in place to determine access rights to data by job duties. Wherever there is a reference within Wayne County policies to the designees of a Department Head being able to authorized access to resources, data or any protected information, it should be understood that assignment of any designee to these duties MUST be documented with the Department of Information Technology and that by doing so, the Department Head acknowledges that he and the designee both understand their role and responsibilities, and agree to abide by all procedure and policies, both documented in this document and in policies, but also in all internal procedures in common practice within the County. If sensitive information is input and stored in third-party/external/vendor programs or databases, it is the responsibility of each County department to monitor the processes by which this is done and to maintain control of the security of the information that it owns.

Information Security Officer's Roles and Responsibilities

Wayne County is a decentralized organization and as such, the Information Security Officer (ISO) role is delegated to individuals within the following departments: Information Technology, E911 Dispatch Center, Emergency Management Services, Public Health Department, Nursing Home, Mental Health Department, Department of Social Services, County Clerk, Department of Motor Vehicles, and Aging and Youth Department. These roles oversee the acceptable use of County owned equipment, security, and integrity of the data in their respective areas.

- The Director of Information Technology is the County ISO responsible for the core technology services provided by the central IT department including disaster recovery specific to the Information Technology department. The Director of Information Technology was designated the Security Officer to satisfy the requirements of HIPAA with the responsibility to oversee computer and system security for matters related to compliance and HIPAA by Resolution **553-13**.

- The E911 Operations Manager is the ISO responsible for Public Safety data associated with the E911 Dispatch Center, Sheriff's Office, and Jail facility.

- The Director of Emergency Management is the ISO responsible for Emergency Management Services data.

- The Director of Public Health is the ISO and HIPAA Compliance Officer responsible for Resident Care data and all other protected or sensitive data associated with the Wayne County Nursing Home.

- The Director of Mental Health is the ISO and HIPAA Compliance Officer responsible for Patient Care data and all other protected or sensitive data associated with the Mental Health department.

- The Commissioner of the Department of Social Services is the ISO responsible for all services data and all other protected or sensitive data associated with the Department of Social Services.

- The County Clerk is the ISO responsible for all protected or sensitive data associated with the Office of the County Clerk.

- The Commissioner of Motor Vehicles is the ISO responsible for all protected or sensitive data associated with the Department of Motor Vehicles.

- The Director of Aging and Youth is the ISO for all protected or sensitive data associated with the Department of Aging and Youth.

- The Director of Information Technology is the ISO for all other departments not specifically mentioned above.

The Information Security Officer's responsibilities include, but are not limited to:

- Developing, deploying, and maintaining an information security architecture that should provide security guidelines, mechanisms, processes, standards, and procedures that meet current and future business needs of the County.

- Providing guidance to the County department regarding security threats that could affect the County computing and business operations, and providing tools and procedures to mitigate the risks associated with these threats.

- Assisting management in the implementation of any additional security measures due to specific business needs of the individual County departments.

- Developing and implementing security training and awareness programs that educate County information users with regard to the County's information security requirements; information users include all County employees and individuals who work under agreements with the County (such as Contractors, Consultants, Vendors, Interns, Research Partners, Volunteers and other persons in similar positions.)

- Investigating and reporting to management breaches of security controls, and implementing additional compensating controls when necessary to help ensure security safeguards are maintained.

- Participating in the development, implementation, and maintenance of disaster recovery processes and techniques to ensure the continuity of the County department's business and the security controls, in the event of an extended period of computing resource unavailability.

County Employees

It is the responsibility of all employees to protect County information and resources, including passwords, and to report suspected security incidents to their Department Head or an assigned designee and the County Information Security Officer. County employees are expected to adhere to the guidelines outlined in the document.

All County Authorized Users are responsible for maintaining the confidentiality, integrity and availability of the County's information to facilitate effective and efficient conduct of County business.

Three responsibility classifications (owner, custodian, and user) are defined to assist County authorized users in understanding their roles and responsibilities when using the County's information systems. County authorized users may fall into more than one category.

Owner: All information residing on the County's information systems is owned by the department that created it. Information owners (County department heads and designees) determine the appropriate information sensitivity classification to be applied to the information. Owners are responsible for deciding which County authorized users will be permitted to access the information, and the uses to which the information will be put.

Custodian: The custodial role is shared by the department owning the information and in the case of information stored or being carried over County networks, Information Technology Services. Information must be protected in accordance with the information owner's access control, data sensitivity and data criticality specifications. At a minimum, the custody involves:

- ensuring that physical security for the equipment involved with information storage, backup, and recovery systems is adequate
- ensuring a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information is maintained
- developing and maintaining a business continuity and contingency plan
- administering access to information as authorized by the information owner
- implementing procedural safeguards and cost-effective controls.

User: The user is an individual authorized access to an information asset by the owner. The user is responsible for using the information only for the intended purpose -- consistent with the information owner's instructions -- and safeguarding the integrity, confidentiality and availability of the information accessed. Users are also responsible for familiarizing themselves and complying with the County's information security policies.

Non-County Employees

Individuals, who work under agreements with Wayne County and/or for a Wayne County department, such as Contractors, Consultants, Vendors, Interns, Research Partners, Volunteers, and other persons in similar positions, are also required to comply with the policies included in this document: The Wayne County Information Security and Accountability Policies and also the Wayne County Compliance Plan Handbook. Wayne County will provide these documents to the vendors and their employees.

Information Technology (IT)

Information Technology management has responsibility for the data processing infrastructure, data, voice, and wireless networks that support the other ISOs and information owners. It is the responsibility of Information Technology management to support these policies, guidelines and procedures and provide resources needed to enhance and maintain a level of information security control that is consistent with this document.

Information Technology management has the following responsibilities in relation to the acceptable use and the security of information:

- Ensuring processes, guidelines and requirements are identified relative to the acceptable use and security requirements defined by the County's business.

- Ensuring the participation of the technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and in protecting information assets.

- Ensuring the appropriate security requirements (as requested by the information owners, the department head, or designee) for user access to digital information are defined for files, databases, and physical devices assigned to their areas of responsibility.

- Provide off-site storage of critical data and periodically test that recovery of back-up media will work, if and when, needed.

Security Policies and Procedures

Purpose: The purpose of this policy is to establish the process by which Wayne County IT Security and Confidentiality Policies meet federal regulations for HIPAA compliance.

General Policy: Wayne County is required to have policies and procedures for compliance with reviewing the HIPAA Security Rule. All policies will be reviewed at least annually and updated as needed.

Policy Documentation

Policies and Procedures

1. New Wayne County IT Security and Confidentiality Policies or revisions to existing may be required due to:
    a. Changes in business practices or the Information Technology (IT) environment of the HIPAA covered components
    b. Mandated federal law enacted by Congress
    c. Risk analysis determines new or increased vulnerability to security threat

2. All policies and procedures implemented to comply with the HIPAA Security Rule shall be made available to the HIPAA covered component workforce, and additionally to all those having access to other sensitive and protected information {as described on page 5 of this document).

3. All actions, activities, or assessments required by the Wayne County IT Security and Confidentiality Policies shall be documented. The documentation shall provide sufficient detail to communicate the implemented security measures and to facilitate periodic evaluations by the HIPAA covered components or as requested by the Wayne County Compliance Officer. In accordance with 45 C.F.R. § 164.316, documentation shall be retained for a minimum of six (6) years from the time of its creation or the date it was last in effect, whichever is later.

Compliance Committee Responsibilities

1. Draft new or updated Wayne County IT Security and Confidentiality Policies as indicated in the Policies and Procedures section above.

2. Communicate the approved new or revised policy to the workforce of the HIPAA covered components, and additionally to all those having access to other sensitive and protected information (as described on page 5 of this document). And also to update training and related materials as needed.

3. Maintain and make available to the workforce the Wayne County IT Security and Confidentiality Policies in electronic form, or hardcopy. This document is posted on the Wayne County intranet for reference.

Compliance Officer Responsibilities

Request final approval of the Wayne County IT Security and Confidentiality Policies from the Wayne County Board of Supervisors for any "significant or material" change.

Acceptable Use

IT SECURITY AND CONFIDENTIALITY POLICY

OVERVIEW: Wayne County ("County") provides a variety of electronic resources to its officers and employees, including but not limited to computers, tablets, smart phones, local and wide area networks, software, internet and email services, etc. Use of these resources and the safeguarding of all protected data in any form or format (including but not limited to electronic, paper and voice), should be guided by common sense, and the purpose of this policy is to define the acceptable limits within which users may exercise their discretion.

PRINCIPLES:

1. All existing County policies and practices apply to all uses of electronic resources and to safeguarding all forms of protected information. These policies and practices include but are not limited to those that deal with intellectual property protection, privacy, misuse of County resources, sexual harassment, information and data security, confidentiality, solicitation on County premises, records retention, open meetings and freedom of information.

2. Users should have no expectation of privacy in their use of County computer resources. The equipment and connections are County property, provided for County purposes, and the County will inspect and monitor internet and email use, as well as other computer uses. **SOFTWARE AND SYSTEMS THAT CAN MONITOR USE WILL BE UTILIZED**. Use of County computer systems and networks constitutes consent to such monitoring and inspection without prior notice.

3. Users shall not apply County resources to personal gain, including but not limited to marketing, sales or solicitation, the advancement of any personal belief or creed, religious or political; to illegal activities of any sort, including but not limited to sexual harassment, prohibited discriminatory activity, or copyright infringement; to threatening, obscene, defamatory or harassing activities; to disruptive, unethical or unprofessional behavior. Users shall not apply County resources to intentionally interfere with the performance of the resources, especially networks; to access data on any device without the owner's permission; to interfere with the legitimate work of other users; to conduct intimate communication; to spread computer viruses, Trojan horses, worms or any other program designed to violate security, interfere with proper operation of any computer system or destroy another user's data; to communicate in the name of the County, or when it may reasonably be assumed that the user is communicating on behalf of the County, without authorization to do so. Users shall not apply County resources to any activity which is not directly related to the operation and conduct of County government.

4. All data, information, records and software on County resources are the property of the County. Data electronically generated by users should not be kept on local hard drives

but on departmentally designated network servers for security, accessibility and backup purposes.

5. Resource security must be maintained, and users shall take precautions, including safeguarding their passwords; maintaining reasonable physical security around County equipment (i.e. home-use or any remote use); and logging off unattended work stations. Personal devices that access County data must be reviewed by the IT Department to ensure that up-to-date virus protection is enabled. **USERS SHALL NOT INSTALL SOFTWARE THAT HAS NOT BEEN AUTHORIZED BY THE Director of Information Technology, NOR ENABLE AUTOMATIC LOGON TO ANY COUNTY RESOURCE.** All incidents potentially affecting system security shall be reported to the Director of Information Technology**.**

6. Emails created in the normal course of official County business and retained as evidence of official County policies, actions, decisions or transactions are records subject to records management requirements under the New York Arts and Cultural Affairs Law, and may be subject to specific program retention requirements. Such records include but are not limited to policies and directives, correspondence or memoranda related to official business, work schedules and assignments, agendas and minutes of meeting, any document that initiates, authorizes or completes a business transaction, final reports or recommendations.

7. Records communicated or transmitted by email shall be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements; retained, managed and accessible in an existing filing system outside the email system in accordance with the appropriate departmental standard practices as may be recommended by the Director of Information Technology; **and disposed of within the record keeping system which they have been filed in accordance with a *Records Disposition Authorization (RDA) approved by the State of New York Archives and Records Administration (SARA), and implemented by the Records Management Officer.***

8. All County employees will use their County provided email address for official correspondence. This ensures official correspondence is retained appropriately.

9. Any violation of these policies could lead to disciplinary action or criminal prosecution, or both.

Acceptable Use of E-mail

Purpose: The purpose of this policy is to safeguard the public image of Wayne County. Use of Wayne County's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of Wayne County. The objectives of this policy are to outline appropriate and inappropriate use of Wayne County's e-mail

systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope: This policy applies to all e-mail systems and services owned by Wayne County, all e-mail account users/holders at Wayne County (both temporary and permanent), and all County e-mail records.

General Policy: E-mail access at Wayne County is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Employees of Wayne County are provided an e-mail account based on job function and business need as determined by the Department Head. E-mail accounts will be granted to third party individuals who work under the agreements with the County (such as Contractors, Consultants, Vendors, Interns, Research Partners, volunteers and other persons in similar positions) on a case-by-case basis. The Department head (or designee) who has contract authority with the third party is responsible for submitting requests for accounts using templates which will be made available on the County internal website.

The standard E-mail form is controlled by settings in Active Directory which include:

- The County's Confidential Notice at the closure of every County email correspondence "This transmission, including any attachments, is for the sole use of the intended recipient(s) or entity named above and may contain confidential and privileged information. If you received this and are not the intended recipient(s), you are hereby notified that any disclosure, copying, unauthorized distribution or the taking of any action in reliance on the contents of this information is prohibited. If you have received this transmission in error, please immediately contact the sender as indicated above to arrange the proper handling of the information."

- Signatures: Wayne County standard form for the signature section shall be limited to name, job title, department, address, phone number, fax number, and email contact information. No extraneous messages, personal slogans or beliefs will be allowed, other than business specific, mission statement material approved by the Department Head and the Director of Information Technology will be permitted.

E-mail users are responsible for mailbox management, including organization and cleaning. Email quotas are determined based on job functions and exist to control email storage costs and ensure the performance of the email application. Once your email quota is reached you must delete/ archive email before the application will allow you to send any more e-mail messages.

Wayne County's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use must not interfere with others' use of Wayne County's e-mail system and services. E-mail use at Wayne County will comply with all applicable laws, all Wayne County policies, and all Wayne County

contracts. E-mail users are expected to comply with normal standards of professional and personal courtesy and conduct.

The following activities are deemed inappropriate uses of Wayne County systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

- Use of e-mail in any way that violates Wayne County's policies, rules, or administrative orders.

- Viewing, copying, altering, or deletion of e-mail accounts or files belonging to Wayne County or another individual without authorized permission.

- Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 10 megabytes or less.

- Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.

- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.

Forwarding: Employees must exercise caution when sending any email from inside Wayne County to an outside network. Unless approved by an employee's Department Head or designee and the Director of Information Technology, Wayne County email will not be automatically forwarded to an external destination. Sensitive information or any information containing EPHU will not be forwarded via any means, unless that e-mail is critical to business and is encrypted in accordance with the information below.

Encryption: Encryption of the e-mail applies to all employees of Wayne County who do business with users outside of the Wayne County network. This process happens automatically. Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis of encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate’s Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or DiffieHellman, while secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be a length that yields equivalent strength. Wayne County currently uses Zix Corp which states as of August 2013 that “Hash functions used in Zix Corp software are derived from the RSA Data Security, Inc., MD-5 Message Digest Algorithms”

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IT. Be aware that the export of encryption technologies is restricted by the U.S. government, Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Sensitive and confidential information needs to be protected against unauthorized parties. The use of good encryption technology can reduce the County's risk of non-compliance. The encryption solution is content-aware and policy-based so e-mails are automatically scanned for sensitive information. If sensitive content is found in the subject line, message body or in attachments, the solution will automatically encrypt, route block or brand the outbound email based on Wayne County policies.

Archiving: Most organizations must archive copies of e-mail messages for legal, regulatory, and/or operational reasons. Wayne County is committed to good business practice and upholding the laws and regulations that govern its operation. E-mail maintained on the County's computers, based on judicial decisions rendered by the state's highest court, constitutes County records and is subject to the rights of access conferred by the Freedom of Information Law. As such, records subject to the Local Government Records Law cannot be destroyed or disposed of until the minimum period for the retention of the records has been reached.

Any e-mail message deemed a 'business record' shall be archived and retained for as long as the law demands. A business record is any print or electronic document created and maintained in the ordinary course of business. However, not every e-mail message constitutes a business record that must be kept. An e-mail and any of its attachments should be retained if it documents business activities that have evidentiary or reference value, or it is the sole copy of the information. This includes, for example, job offers, contract negotiations where final pricing is set, or a policy memo. It does not include, for example, in-progress drafts, discussions, or negotiations; received copies of policy memos where an original already exists; or non-business correspondence. This policy applies to the email system provided by Wayne County and to all County employees and anyone using a Wayne County email account.

Any e-mail message deemed a 'business record' that is required by law to be stored for legal reviews and/or audits will also be archived and retained for as long as the law demands. These e-mail messages will also be disposed of in accordance with any regulations governing Wayne County and the industry in which it resides.

Any and all archived e-mails will be tagged with meta data in order to make e-mail headers, content, attachments, and text fully searchable. In addition, Wayne County will deploy and maintain technology that supports the long term retention, archiving and search ability of stored e-mail messages.

As such, Wayne County's Information Technology department has deployed Mail Archive software. The software will store ALL inbound and outbound e-mail messages for a period of 7 years. The long term retention and storage of e-mail business records that require longer than

a 7-year retention period in accordance with any regulations governing Wayne County and the industry in which it resides is the responsibility of individual departments who send and/or receive the e-mail message. If a department has a need to keep past 7 years they need to notify the Director of Information Technology of the requirement.

If litigation against Wayne County or its employees is filed or threatened, the law imposes a duty upon the County to preserve all documents and records that pertain to the issues. The County Attorney will notify the appropriate individuals if litigation is pending or threatened and provide direction as to what documents need to retained and the method for the retention. This is referred to as a 'litigation hold' and this directive overrides any and all e-mail retention policies.

Acceptable Use of Office Telephones

Purpose: Telephone communication is an essential part of the day-to-day operations of Wayne County. Telephone and voicemail services are provided to employees in order to facilitate performance of work. The goal of this policy is to balance the business need for telephone and voicemail use with the costs involved.

Scope: This policy applies to all employees of Wayne County, and all usage of County provided land line phones, VOIP, and cellular/mobile devices, voicemail, and fax services.

General Policy: As with all Wayne County resources, the use of telephones, voicemail and fax services should be as cost effective as possible and in keeping with the best interest of the County. All employees must operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Wayne County.

- The information Technology department is responsible for installation and repair of all County telephony equipment and administration of telephone and voicemail accounts with the exception of the e911 Dispatch Center. The Director of Emergency Management is accountable for this operation.

- Department Heads or their assigned designee are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring IT is notified of any additions, moves, or changes required to telephone and voicemail services. Service request should be submitted using the appropriate template available on the County's internal website.

- The County is charged for each **EXTERNAL** telephone call made or fax sent so the number of telephone calls made should be limited in number and duration to that necessary for effective conduct of business.

- All voicemail boxes will be protected with a PIN (personal identification number). PINs should be changed every 90 days to aid in mailbox security. Easy-to-guess or previously used PINs will be blocked from the system. PINs must not be shared with others.

- Voicemail is to be used as a backup in the event you are not available to answer a call, and should not be used to “screen” calls. Each user is expected to respond to voicemail messages in a timely manner.

- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts, if applicable.

- Use of directory assistance (i.e. 411) should be avoided since a fee is incurred with each use. If you are unsure of a number, please consult a print or online telephone directories first.

Unacceptable Use

Wayne County telephone, voicemail or fax services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.

- Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.

- Using the telephone system or breaking into a voicemail box via unauthorized use of a PIN or other password.

- Broadcasting unsolicited personal views on social, political, or other non-business related matters.

- Soliciting to buy or sell goods or services unrelated to Wayne County.

- Calling 1-900 phone numbers.

- Making personal long-distance phone calls without permission from their Department Head or assigned designee.

Misuse of telephone and voicemail services can result in disciplinary action, up to and including termination.

Limited Personal Acceptable Use

In general, personal use of telephone, voicemail or fax services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed in guidelines set by the Department Head.

- An employee's work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.

- Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).

- The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.

- The employee needs to make arrangements for emergency repairs to his or her residence or automobile.

- A call that reasonably could not be made at another time and is of moderate duration.

If a personal long-distance call must be made that will be billed to Wayne County, the employee should receive permission from their Department Head or assigned designee first. Regardless, employees are expected to reimburse the County for the cost of any long-distance calls within 30 days of receipt of the relevant bill.

Monitoring
Wayne County reserves the right to monitor telephone, voicemail and fax use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

Voice Mail Retention
Voice Mail messages are not systematically retained on the voice mail system. Retention of voice mail messages are controlled by each individual voice mail subscriber. If a message is deleted the day it is received, they no longer exist and cannot be retrieved by anyone. If a message has not been deleted before the nightly back-up, it is retrievable for up to 14 days. The voice mail system configuration is also periodically backed up.

Service and Repair
The IT Department requires 5 business days' notice to set up a standard telephone service and voicemail box. If there is a problem with an existing telephone or voicemail box, contact the IT Department by emailing support@co.wayne.ny.us. Users who do not have access to email should have a co-worker email on their behalf.

Acceptable Use of Printers and Copiers

Purpose: Printers and copiers represent one of the highest equipment expenditures at Wayne County. The goal of this policy is to facilitate the appropriate and responsible business use of printer and copier assets, as well as control these cost of ownership by preventing the waste of paper, toner, ink, etc.

Scope: This Printer and Copier Policy applies to all employees of Wayne County as well as any contract employees in the service of the County who may be using this equipment.

General Policy:

- Printers and copiers are to be used for documents that are relevant to the day-to-day conduct of business at Wayne County. Printers and copiers should not be used to print personal documents.

- Installation of personal printers is **generally** not condoned at Wayne County due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is at issue, personal printers may be allowed.

- Do not print multiple copies of the same document -the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the copier to make additional copies or send the entire output to a networked copier.

- If you print something to a common network attached printer/ copier, pick it up in a timely fashion. If you no longer want it, dispose of it appropriately (i.e. recycle).

- If the document you print is confidential in nature, then utilize the private print option that is available on the copiers

- Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers/ copiers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
- Make efforts to limit toner use by selecting light toner and lower dpi default print settings.

- Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer/ copier. If printing a job in excess of 25 pages, be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).

- Printing e-mail messages is discouraged. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.

- Avoid printing a document just to see what it looks like. This is wasteful.

- Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult the printer guide (available on line from manufacturer websites) as to which machines can handle these specialty print jobs or utilize the ***County print shop.***

- Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. Avoid printing in color when monochrome (black) will do.

- If you encounter a physical problem with the printer/ copier (paper jam, out of toner, etc.) and are not "trained" in how to fix the problem, please do not try. Instead, report the problem to the IT Help Desk or ask a trained co-worker for help.

- Any malfunction of a Toshiba copier should be reported directly to the contractor - the service phone number is labelled on the copier, along with the unit's serial number. If the technician replaces the hard drive on the copier, the user should email this information to the IT Help Desk (support@co.wayne.ny.us).

- Report any malfunction of any other print device to the IT Help Desk (support@co.wayne.ny.us).

Acceptable Use of Mobile Devices

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for users who have legitimate business requirements to access County data from a mobile device connected to an external network outside of Wayne County's direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/netbook/tablet computers.
- Mobile/cellular phones, air cards and GPS devices
- Smartphones, etc.
- Devices not owned by the County used to access County resources.
- Any mobile device capable of storing County data and connecting to an unmanaged network.

Scope: The policy applies to any hardware and related software that could be used to access County resources, even if said equipment is not County sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within Wayne County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the County's public image. Therefore, all users employing a mobile device connected to an external network outside of Wayne County's direct control to backup, store, and otherwise access County data of any type must adhere to County-defined processes for doing so.

This policy applies to all Wayne County employees, including full and part-time staff, and individuals who work under the agreements with the County {such as Contractors, Consultants, Vendors, Interns, Research Partners, volunteers and other persons in similar positions), and other agents who utilize either County-owned or personally-owned mobile device to access, store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust the County has built with its clients, supply chain partners and other constituents. Consequently, employment at Wayne County does not automatically guarantee the initial and ongoing ability to use these devices to gain access to County networks and information.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

Connectivity of all mobile devices will be centrally managed by Wayne County's IT department and will utilize authentication and strong encryption measures. Although IT is not able to directly manage external devices - such as home PCs-which may require connectivity to the County network, end users are expected to adhere to the same security protocols when connected to non-County equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the County's infrastructure.

General Policy: It is the responsibility of any employee of Wayne County who uses a mobile device to access County resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Based on this, the following rules must be observed:

- IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the County infrastructure. IT will engage in such action if it feels equipment is being used in a way that puts the County's systems, data, or users at risk.

- Laptop computers or personal PCs may only access the County network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required.

- Smart mobile devices such as smartphones and PDAs are not permitted access to the County network, except for use of email.

- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data

- In the event of a lost, stolen or damaged mobile device, the authorized user must notify both their department head and the IT department immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

Cell phones and mobile broadband devices: Service for all cell phones and mobile broadband devices shall be acquired through the Information Technology Department and in accordance with standard County procurement procedures, through New York State OGS Contract or if it applies, County issued contracts. The requesting department shall work with the IT Department and the designated vendor to determine the appropriate equipment and level of service based on a demonstrated business need.

A County provided cell phone or air card shall be used for appropriate business purposes. Only County staff and other authorized persons conducting County business may use this equipment. Use of this equipment that hinders productivity, interferes with County use or is excessive is prohibited.

A County provided cell phone or mobile broadband device, may be used for personal reasons in an emergency situation or circumstances, whether incoming or outgoing calls, in which an employee must make/receive a personal call, does not have access to a personal device and such circumstance are at the County's request and/or relate to County Business. Be aware that personal use of a County provided mobile device could be considered taxable/reportable income by the Internal Revenue Service (IRS). All telephony Invoices should be reviewed by department heads to determine compliance with IRS Code.

Employees are responsible for taking proper care of mobile devices and reasonable precautions against damage, loss or theft. Loss of mobile devices should be reported to the Department Head immediately. Losses attributed to negligence will be compensated for by the employee at replacement cost.

With the exception of Law Enforcement Officers and Emergency Management Personnel in the case of emergency, employees are prohibited from using any mobile device while operating County or personal vehicles, heavy machinery or equipment.

The use of hands free devices or accessories, for non-emergency employees, is required.

Acceptable Use of the Internet

Purpose: The goals of this policy are to outline appropriate and inappropriate use of Wayne County's Internet resources, including but not limited to the use of browsers, electronic mail and instant messaging, file uploads and downloads, and voice communications.

Scope: Internet access at Wayne County is controlled through individual user accounts and passwords. Department Heads or an assigned designee are responsible for defining appropriate Internet access levels for the people in their department and conveying that information through the appropriate template available on the County's internal website.

General Policy:

Individual Internet use will not interfere with others' productive use of Internet resources. Internet use at Wayne County will comply with all Federal and New York State laws, all Wayne County policies, and all Wayne County contracts. This includes, but is not limited to, the following:

The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses). The Internet may not be used in any way that violates Wayne County's policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of Wayne County, misrepresents Wayne County, or violates any Wayne County policy is prohibited.

- Wayne County prohibits use for mass unsolicited mailings, access for non-employees other than individuals who work under the agreements with the County (such as Contractors, Consultants, Vendors, Interns, Research Partners, volunteers and other persons in similar positions) to Wayne County resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, competitive commercial activity and the dissemination of chain letters.

- Individuals may not establish County computers as participants in any peer-to-peer network, unless approved by management.

- Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Wayne County or another individual without authorized permission.

- In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business purposes.

- Individuals will only use Wayne County-approved services for voice communication over the Internet.
- Video services such as TeleHealth, WebEx and GoToMeeting will be allowed on an as needed basic and may be revoked if misused.

Security: For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the Help Desk or IT Administrator to obtain password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to internet services.

Monitoring and Filtering: Wayne County may monitor any Internet activity occurring on Wayne County equipment or accounts. Wayne County currently does employ filtering software to limit access to sites on the Internet. If Wayne County discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

Acceptable Use of Social Media – County Related

Purpose: Wayne County desires to operate and maintain its social media sites as a public service to convey important, valuable and possibly urgent information about County programs, services, projects, issues, events, activities, as well as, health and safety alerts and updates to an increasing mobile population. The Board of Supervisors and the County Administrator have an overriding interest and expectation in deciding who may "speak" and what is "spoken" on behalf of Wayne County on social media sites. This policy establishes guidelines for the use of social media.

Scope: This policy applies to all social networking technologies including but not limited to Facebook, MySpace, Twitter and LinkedIn that are accessed using a Wayne County email address. Employees are responsible for the on line activities that are conducted with a Wayne County email address.

General Policy: This policy addresses, employee access at work to monitor social media and maintenance of official County social media sites by County employees.

A Wayne County employee may only use social networking technologies if authorized by his or her Department Head and the Director of Information Technology. Otherwise, accessing social networking from a Wayne County computer is prohibited.

Departments permitted to set up an official social media site will be required to ensure the site remains up-to-date to ensure that offensive or non-factual comments are removed as soon as possible after posting. Commenters leaving inappropriate post must be immediately blocked

from posting to the site in the future. It is the responsibility of Department Heads to ensure the accuracy of all information posted on their department's sites.

Employee Access
Employee access to social media will be granted on a case by case basis and only when the County determines there is a genuine business need. Access to streaming video sites including YouTube, even though for work, may be subject to brief and temporary access. Streaming video requires a great deal of bandwidth and extensive use within the County can be expected to place a strain on the network bandwidth available for Internet access by user Countywide.

Department Heads interested in using Social Media for official purposes must prepare a Business Case Justification for approval. The Business Case Justification is to be submitted to the County Administrator, County Attorney, Director of IT and submitted to the appropriate committee for approval. At minimum, the business case will:

- Name the Social Media outlet to be utilized (i.e., Facebook, Blog)
- State the goals for setting up a Social Media Site
- Identify the intended audience
- Summarize the type of information expected to be shared/displayed
- Discuss the anticipated benefit from establishing the site
- Provide the names, titles and role for each department employee expected to administer the site. Designated employees of Information Technology must also be given administrative rights to the site to ensure the site can be taken down at any point that the Department Head or County Administration determines appropriate.
- Include a declaration signed by the Department Head indicating their explicit understanding that they remain ultimately responsible for monitoring their department's official site and that they will ensure it is maintained in a manner that is proper, prudent and complies with all County policies, state, federal and local laws.

Account Management
Once a Department Blog or Facebook page or other social media account has been approved, the department will be given appropriate internet access to be able to set up the site. It will be the responsibility of those employees identified in the Business Case Justification to administer the site. It is very important that all site content remain current, accurate and pertinent to County topics. Departments are responsible for establishing and maintaining content posted to their social media page and shall have measures in effect to prevent inappropriate or technically harmful information, media content, and links. Social media pages are not intended to be used in a way that guarantees the right to free speech. Each department is responsible

for monitoring these postings, and taking appropriate action when necessary, to protect general site visitors from inappropriate or technically harmful information and links. Departments with a Social Media site are encouraged to identify at least 3 Administrators so that site monitoring can be better covered during employee vacations or illness.
Written notification of changes in the Administrators for any social media site must be promptly provided to the Information Technology Department by the Department Head or designee through the appropriate template available on the County's internal website. This documentation shall be kept on file with the approved Business Case Justification for audit purposes. The Information Technology Internet filter will be adjusted accordingly and access to Social Media on the County network will be initiated or terminated as appropriate.

Acceptable Use
Access to Social Networking will be provided to a limited number of County employees under this policy and for the sole purpose of maintaining a department's site. Maintaining an official County Social Media site will be considered an official job responsibility for each Administrator and they will be allowed to do this on County time. Administrators may not check on nor comment on their personal Facebook or other Social Media page or on the pages of friends during work hours.

Employee Conduct
Requirements for employee conduct on Social Media on County time include but are not limited to the following:

- Protection and respect of the public we serve will remain paramount
- Keep interactions factual and accurate
- We will strive for transparency and openness in our interactions and will never seek to "spin" information for personal benefit
- Links to credible sources of information to support interactions will be provided whenever possible
- We will publicly correct any information we have communicated that is later found to be in error
- We will be honest about our identity
- We will respect the rules of the social media outlet being utilized
- We will always protect privacy and permissions

It is recognized that employees may access Social Media on their own personal time to conduct "concerted activities" related to their terms and conditions of employment, as defined in the relevant labor laws, or to conduct activities protected by the First

Amendment. Even while accessing Social Media on their own personal time, employees will not defame anyone, including but not limited to their supervisors or managers, and will not disclose confidential information of the County, its clients, partners, vendors and suppliers, including but not limited to trade secrets or proprietary information.
Anyone found to be non-compliant with the policy stated here when commenting either officially or unofficially on Social Media shall be considered disciplinary action in accordance with relevant law and/or the relevant Collective Bargaining Agreement, up to and including termination of employment.

Content
Content and comments posted on each department site are expected to be restricted to topics appropriate to the mission of that department. Content is to remain factual and at no time shall employee opinions be posted on a County department site. Inappropriate content will not be tolerated and socially unacceptable comments are to be removed immediately upon discovery. Questions or comments from the public that are not related to the department mission are to be referred to the appropriate County department for action. All social media and/or networking websites shall clearly indicate they are maintained by Wayne County and shall have the County contact information prominently displayed. Wherever possible, links should direct users back to the County's official website for more information, forms, documents, or online services necessary to conduct business with Wayne County.

Risks
As indicated in the **New York State Office of Cyber Security and Critical Infrastructure Coordination "Secure Use of Social Media" Guidelines**, Cyber criminals target social media sites because they offer an effective means of propagating malicious code to a wide and generally unsuspecting audience. Sites that allow user-generated content {i.e., Facebook) are among the most active distributors of malicious content, such as worms that can shut down networks, or spyware and keystroke loggers that can compromise County data. Many postings are spam or contain malicious links that are not apparent to the user.

To help guard against these risks, users must remain mindful when interacting on Social Media. Employees and other users representing Wayne County Government must:

- Never divulge Personal, Private or Sensitive Information (PPSI) pertaining to the County, themselves, another employee, a contractor or vendor or any consumer or member of the public as they are associated with Wayne County. PPSI includes but is not limited to a person's name, bank account numbers, credit card numbers, driver's license numbers, a person's health condition or any meeting, evaluation or event related to any other type personal information related to an individual or department.

- Never click on a link that you are not absolutely sure is credible

- Comply with all Wayne County IT policies including all Wayne County IT Security and Confidentiality Policies

If a department site Administrator is concerned that they may have inadvertently clicked the wrong link and have downloaded malicious code, they are to immediately disconnect their PC from the network by unplugging **the blue cord**. After the PC is disconnected, they are to contact the IT Helpdesk by calling 946-7450. The network cord must remain unplugged from the PC until cleared by IT.

Legal Issues
All Wayne County social networking sites shall adhere to appropriate Wayne County Policies, including but not limited to the Wayne County Personnel Rules and the Wayne County Code of Ethics. These sites must comply with all applicable federal, state, and local laws and procedures including, but not limited to copyright, records retention, NYSFOIL, privacy laws and HIPAA. Users who fail to observe such policies and laws will be subject to the sanctions imposed by that policy or law.

Citizen Conduct
Wayne County Social Media sites shall each include a notification to visitors that the intended purpose of the site is to serve as a mechanism for communication between Wayne County departments and the general public. Wayne County social media posts in the form of questions or comments containing any of the following forms of content shall not be allowed and shall be removed immediately upon discovery:

- Comments not related to the particular social article being commented upon
- Comments in support of or opposition to political campaigns
- Profane language or content
- Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation
- Sexual content or links to sexual content
- Solicitations of commerce
- Conduct or encouragement of illegal activity
- Information that may tend to compromise the safety or security of any individual or the general public, or
- Content that violates a legal ownership interest of any other party

These guidelines must be displayed to users or made available to them via a prominently displayed hyperlink on the department site. Any content removed based on a violation of these guidelines must be retained and kept on file by the department, including the time, date, and

identity of the poster when available. The Administrator discovering and removing the post shall also be identified in the file documentation of the incident.

Acceptable Use of Social Media – Personal

Purpose: At the Wayne County, we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media. This policy applies to all employees who work for the Wayne County.

GUIDELINES

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, or the comments section of an online news story, whether or not associated or affiliated with Wayne County, as well as any other form of electronic communication.

Ultimately, you are solely responsible for what you post on line. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees or otherwise adversely affects customer, contracted practitioners, suppliers, or people who work on behalf of Wayne County business interests may result in disciplinary action up to and including termination.

Wayne County supports its employees' First Amendment rights, as well as the right of its employees to organize and communicate online. However, Wayne County cannot condone its employees behaving in a manner which negatively impacts the ability of the County to fulfill its mission.

KNOW AND FOLLOW THE RULES

Carefully read, such that you know what is contained in these guidelines: The Wayne County Ethics in HR Policy, **the Wayne County Computer Use Policy**, the Wayne County Compliance Policy, and the Wayne County Sexual Harassment Policy. Ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

BE RESPECTFUL

Always be fair and courteous to fellow employees, customers, contracted practitioners, vendors, or people who work on behalf of Wayne County. Also, keep in mind that you are more likely to resolve work related complaints by speaking directly with your co-workers or by utilizing our "open door policy" than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticisms, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating that disparages customers, employees, contracted practitioners or vendors, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or by County/Department policy.

BE HONEST AND ACCURATE

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Information posted in error and later corrected may still be cause for disciplinary action. Never post any information or rumors that you know to be false about Wayne County, fellow employees, customers, contracted practitioners and vendors, and people working on behalf of Wayne County.

POST ONLY APPROPRIATE AND RESPECTFUL CONTENT

- Maintain the confidentiality of the Wayne County customers and any private or confidential information. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

- Do not create a link from your blog, website or other social networking site to a Wayne County website without identifying yourself as a Wayne County employee.

- Express only your personal opinions. Never represent yourself as a spokesperson for Wayne County. If Wayne County is a subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of Wayne County, fellow employees, customers, contracted practitioners, vendors or people working on behalf of Wayne County. If you do publish a blog or post on line related to the work you do or subjects associated with Wayne County, make it clear that you are not speaking on behalf of Wayne County. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Wayne County."

- Do not create or share content that is obscene or profane. Additionally, do not share content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, military status, national origin, physical or mental disability, genetic information, or sexual orientation, or status as a victim of domestic violence. To do so may result in discipline up to and including termination of employment.

USING SOCIAL MEDIA AT WORK
Use of social media shall not be tolerated while on work time or on equipment we provide, unless it is work-related as authorized by your Department Head or assigned designee. Do not use the Wayne County or State e-mail addresses to register on social networks, blogs or other on line tools utilized for personal use. Individuals shall only use social media sites during work hours, including on their personal cellular telephone or other communication device, for business-related purposes.

RETALIATION IS PROHIBITED
Wayne County prohibits taking negative action against any employee reporting a possible deviation from this policy or for cooperating in an investigation. Any employee, who retaliates against another employee for reporting a possible deviation from this policy, or for cooperating in an investigation, will be subject to disciplinary action, up to and including termination.

MEDIA CONTACTS
Wayne County employees should not speak to the media (for example, newspapers or radio stations) on the County's behalf without contacting the County Administrator and/or County Attorney. All media inquiries should be directed to them.

Authentication and Password Management

Purpose: Passwords are an important component of information and network security. The use of a Network-ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to provide the guidelines necessary for all of the employees of Wayne County (including individuals such as Contractors, Consultants, Vendors, Interns, Research Partners, volunteers and other persons in similar positions) to create appropriate passwords and to use them and protect them in an appropriate manner. Workforce members will select strong passwords to authenticate their access to information systems that may contain electronic protected health information (EPHI) and other sensitive and protected information (see page 5 of this document), and they will keep these passwords secure and private and not share them with others.

Scope: This policy applies to all users of Wayne County networks and resources.

General Policy: Resolution 177-10 Wayne County Password Policy went into effect March 16, 2010 to ensure the security and integrity of the network, each user is provided with a user account to access network resources. Each user account consists of a unique user ID and password and allows Wayne County to hold users accountable for their activities on the network. Users must not share their password with anyone, and will be held responsible for activities associated with their account. Under this policy, users of the Wayne County IT network will be required to change their passwords every 45 days.

If a user is locked out or cannot remember their password for access to the Wayne County network they can use the password self-serve program linked on the County login page. If this is not possible they can request another user to send an e-mail to support@co.wayne.ny.us requesting that the password be reset, including the employee's name and phone number where they can be reached. The Department Head or their designee are responsible for communicating to their users any requirements for establishing and maintaining passwords for password-protected applications used within their department.

The password must meet the length rule requirements. The password must contain at least: 8 Characters. The password length is not limited. The password must not contain more than 3 characters repeated in succession, 3 identical characters, and no characters in direct or inverse numerical or alphabetical order. The check is not case sensitive. The password must meet not contain all or part of the user's account name. It must contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)
- Non-alphabetic characters (such as !, $, #, %)

The password must meet the password history requirements of the system. The number of passwords to store: 10. The password must meet the password maximum age requirements of the system. Maximum password age: 45.

Data Backups

Purpose: This policy refers to the system level back up and retention of data that resides on Wayne County servers.

Scope: This policy pertains to data stored on County supported servers. Users MUST save their data to the appropriate network drive (home folder or shared folder on a file server) in order that all data is backed up regularly in accordance with this policy.

General Policy: The backup and retention of information stored on County supported servers is the responsibility of the Department of Information Technology. All servers (except servers supporting the camera systems) have a full system (entire server) backup run daily. Data is

retained for seven years. Data on camera servers is kept for a standard period of time before being overwritten.

Device Media Controls

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for users who have legitimate business requirements to connect ANY TYPE of portable removable media to any infrastructure within Wayne County's internal network(s) or related technology resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media

.

- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.
- PDAs, cell phone handsets, and Smartphone's with internal flash or hard drive-based memory that support a data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (Wi-Fi, WiMAX, IrDA, Bluetooth, among others) or wired network access.

Scope: The policy applies to any hardware and related software that could be used to access County resources, even if said equipment is not County sanctioned, owned, or supplied.

This policy applies to all Wayne County employees, including full and part-time staff, and individuals who work under the agreements with the County (such as Contractors, Consultants, Vendors, Interns, Research Partners, volunteers and other persons in similar positions) and any other agents.

General Policy: It is the responsibility of any user of Wayne County networks or technology, who is connecting a portable storage device, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is

imperative that any portable memory that is used to conduct Wayne County business be utilized appropriately, responsibly, and ethically.

The following rules must be observed:

- The IT Department reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to County and County-connected infrastructure.
- End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain County data.

- Protected information should be interpreted as inclusive of all types of sensitive information, whether or not that is explicitly mentioned. This includes but is not limited to: Personal or private information (PPI), Protected Health Information {PHI}, Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII), financial information AND electronic and hardcopy protected or private information. If there is a legitimate business requirement for protected information to be placed on a portable storage device, County approved, encrypted media must be obtained from the IT Department.

- Wayne County's IT department will support sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media.

- IT reserves the right to physically disable USB ports to limit physical and virtual access and reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

Protection from Malicious Software

Purpose: The purpose of this policy is to establish criteria for protections to guard against, detect, and report malicious software. Malicious software includes, but is not limited to, viruses, worms, malware, and spyware.

Scope: This policy applies to all computers that are connected to the Wayne County network via a standard network connection, wireless connection, modem connection, or VPN (virtual private network) connection.

General Policy: Wayne County shall ensure all workstations install and maintain current anti-virus software. All workstations shall be configured to activate and update anti-virus software automatically. In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation that poses a significant risk that equipment shall be disconnected from the network until it has been appropriately cleaned.

Workforce Member Responsibilities

1. Disabling automatic virus scanning features is prohibited.

2. Personal devices that access County data must be reviewed by the IT Department to ensure that up-to-date virus protection is enabled. Only County owned or IT Department approved devices may connect to the County network using VPN.

3. The Department Head or assigned designee and the IT Department must be contacted immediately if a virus is suspected. (see the ***Breach Notification Policy***)

IT Support Responsibilities

1. Maintain current anti-virus software on all workstations.

2. Configure laptops to activate and update anti-virus software automatically when connected to the County network.

3. Inform the Department Head or assigned designee of any new virus, worm, or other malicious code that may be a threat to any protected information (as described on page 5 of this document), who will then inform the IT department.

4. Disconnect any server or workstation from the network until it has been appropriately cleaned if it is infected by a virus, worm, or other malicious code posing a threat to any protected information.

Department Head/Designee Responsibilities

Ensure that ALL devices (PCs, laptops, tablets, etc.) are routinely connected to the network so that updating of antivirus protection and also Windows and program upgrades can occur.

Anti-Virus Process Guidelines

Recommended processes to prevent virus problems are as follows:

- Never disable the County-supported anti-virus software.

- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash bin.

- Delete spam, chain, and other junk email without forwarding, in accordance with Wayne County's Acceptable Use Policy

- Never download files from unknown or suspicious sources.

- Do not store any protected information (as described on page 5 of this document) on a portable storage device unless there is absolutely a business requirement to do so, and if so, use County-approved, encrypted media obtained from the IT Department.

- Always scan mobile storage devices from an unknown source for viruses.

- Users MUST save their data to the appropriate network drive (home folder or shared folder) so that all data is backed up regularly and can be recovered if needed.

Risk Analysis and Management

Policy: The purpose of this policy is to establish periodic evaluations of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (EPHI) held by Wayne County and to manage the security of the EPHI by identifying, controlling, and mitigating risks. Note: while this policy was developed specifically to meet HIPAA regulations, the rules developed at Wayne County should always be applied to all protected information (see page 5 of this document): protected information should be interpreted as inclusive of all types of sensitive information, whether or not that is explicitly mentioned. This includes but is not limited to: Personal or private information (PPI), Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII), financial information AND electronic and hardcopy protected or private information.

General Policy: Wayne County shall perform risk analysis and management through periodic assessments and implementation of controls to mitigate risks.

Risk Analysis

In order to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the EPHI held by Wayne County, the following activities shall be conducted and documented:

1. Periodic program assessments including a security review of facility access controls, document destruction, and protection of network/server closets, workstations and portable devices.
2. Assessments of new or existing information system applications that contain, or are used to protect EPHI and other protected information.
3. Assessments of modifications to existing facilities or development of new facilities that maintain or house EPHI and other protected information.
4. Assessments of new programs, departments, or changes in the mode or manner of service delivery involving EPHI and other protected information.

Risk Management

Security measures and controls, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, shall be implemented:

1. Workforce security training and awareness reminders
2. Access controls, authorization, and validation procedures
3. Detection and activity reviews
4. Applications and data criticality analysis
5. IT systems change management
6. Incident reporting and response procedures
7. Sanctions for non-compliance
8. Contingency, Data backup, and **Disaster Recovery Planning**

IT Change Management

The risk management process shall include change controls for all alterations that occur in the information systems that support, contain, or protect EPHI. These alterations include but are not limited to:

1. Installation, update, or removal of network services and components
2. Operating system upgrades
3. Installation, update, or removal of applications, software, and database servers

IT change management notification and implementation shall follow the policies and procedures as documented by IT support.

Log-in Monitoring

To ensure that access to servers, workstations, and other computer systems containing electronic protected health information (EPHI) or any other protected or sensitive information (see page 5 of this document) is appropriately secured, the following log-in monitoring measures shall be implemented:

1. A mechanism to record all failed log-in attempts on network systems containing EPHI when the technology is capable. To the extent that technology allows, a means to

disable any User ID that has more than four consecutive failed log-in attempts within a 30-minute period.
2. A review of log-in activity reports and logs when required to identify any patterns of suspicious activity, such as continuous failed log-in attempts.

Information System Activity Review

Information system activity reviews and audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources.
2. Investigate possible security incidents to ensure compliance with Wayne County Information Technology (IT) and security policies.
3. Monitor user or system activity as required.
4. Verify that software patching is maintained at the appropriate security level.
5. Verify that virus protection is current.

Information System Audit Controls

To ensure that activity for all computer systems accessing EPHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, IT support staff shall review audit logs, activity reports, or other mechanisms for indications of improper use.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with EPHI shall be archived and protected from unauthorized access, modification, and deletion.

IT Support Responsibilities

1. Inform the Office of Compliance of the planned installation, update, or removal of any application containing EPHI in a HIPPA covered component.
2. Implement and manage the log-in monitoring and audit controls through activity reports on systems containing EPHI to comply with the HIPPA Security Rule.
3. Report all suspicious log-in or system activity to management for investigation and follow-up.

Department Head/Designee Responsibilities

1. Work with IT Support to ensure that user and system activity reports provide sufficient information to determine if improper use of EPHI has occurred.
2. Work with IT Support to investigate reports of potential misuse of log-in accounts or access to EPHI by their workforce.

Risk Assessment Tool

Department Area: _____ Date of Assessment: _____

1. The Security Officer will perform a Walk Around to observe for the following criteria
2. If found to be compliant, YES will be indicated. If found to be out of compliance, NO will be indicated. If NA, NA will be indicated.
3. For any NOs, an assessment will be made by the Security Officer and Department Head as to the Type of Improvement Needed. The QI Committee may also be consulted for improvement opportunities. The following potential improvements will be assessed:
   E=Requires Environmental Change
   P=Requires Process Change
   S=Requires System Change
4. Comments/Recommendation will be made and documented as appropriate.
5. Based on the findings of the assessment, IT will be consulted for recommendations as indicated.

Observation Criteria	YES/ NO/ NA	Type of Improvement Needed	Comments/Recommendations
Security			
Restricted areas and/or files are locked			
Public access is limited at workstations			
Presence of shredders and/or blue recycling containers			
Shredders and/or blue recycling containers easily accessible			
Verbal			
No conversations in public areas with patient information			
Private telephone			

conversations are in private locations			
No staff having confidential conversations in non-private areas (elevators, hallways, etc.)			

Observation Criteria	YES/ NO/ NA	Type of Improvement Needed	Comments/Recommendations
Written			
No papers with PHI in areas where viewable by others			
No PHI in regular trash			
Computers			
Computer screens are shielded or located in a manner that prevents access by unauthorized personnel			
Programs with PHI are exited and the employee is logged off when computer is left unattended			
Email messages contain a confidentiality statement			
HIPPA screen savers on computers			
Printers			
Print jobs are retrieved promptly			

Signature of Security Officer/Designee: _____

Reviewed with: _____on_____

Reviewed with IT?

_____ Yes

_____No

Actions:

Follow up completed by: _____ Date_____

User Access Management

Purpose: The purpose of this policy is to establish rules for authorizing access to the computing network, applications, workstations, and to areas where electronic protected health information (EPHI) is accessible. The HIPAA covered components shall ensure that only workforce members who require access to EPHI for work related activities shall be granted access and when work activities no longer require access, authorization shall be terminated. Note: while this policy was developed specifically to meet HIPAA regulations, the rules developed at Wayne County should always be applied to all protected information (see page 5 of this document): protected information should be interpreted as inclusive of all types of sensitive information, whether or not that is explicitly mentioned. This includes but is not limited to: Personal or private information (PPI), Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII), financial information AND electronic and hardcopy protected or private information.

Scope: In section §160.103 of the HIPAA Privacy Rule, the "workforce" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

General Policy:

Management and Access Control

Only the workforce member's Department Head or an assigned designee can authorize access to the Wayne County information systems. This will be done using templates which will be available on the County internal website in order to facilitate these, and other requests. Any type of request for which a template has been made available must be made through that means.

Access to the information system or application may be revoked or suspended, consistent with Wayne County policies and practice, if there is evidence that an individual is misusing information or other resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measure.

Minimal Necessary Access

Wayne County shall ensure that only workforce members who require access to Electronic Protected Health Information (EPHI) and other sensitive and protected information (see page 5 of this document) are granted access.

Each Department Head or their designee is responsible for ensuring that the access to EPHI and other sensitive and protected information granted to the workforce member is the minimum necessary access required for each work role and responsibilities.
If the workforce member's need for access changes, due to changes in job duties or termination, it is the responsibility of the Department Head or their designee to complete the necessary process to terminate access, through use of the appropriate template.

Granting Access to EPHI

Screen Workforce Members Prior to Access

The Department Head or their designee shall ensure that information access is granted only after first verifying that the access of a workforce member to EPHI and other sensitive and protected information is appropriate.

Sign Security Acknowledgement

Prior to being issued a User ID or logon account to access any EPHI or other sensitive and protected information, each workforce member shall read, and sign the Wayne County IT Security and Confidentiality Policy indicating they agree to the requirements stated before access is granted to the network or any application that contains such information, and thereafter shall comply with all Wayne County security policies and procedures.

Security Awareness Prior to Getting Access

Before access is granted to any of the various systems or applications that contain EPHI or other sensitive and protected information, the Department Head or their designee shall ensure that workforce members are trained to a minimum standard including:

1. Proper uses and disclosures of the EPHI or other sensitive and protected information stored in the systems and/or application
2. How to properly log on and log off of the systems and/or application
3. Protocols for correcting user errors
4. Instructions on contacting a designated person or help desk when EPHI or other sensitive and protected information may have been altered or destroyed in error
5. Reporting a potential or actual security breach

This should also be covered on an annual basis as a refresher in all departments that handle EPHI or other sensitive and protected information, along with in-service type or e-learning for departmentally specific applications.

Department Heads and Designees/Information Owners:

Should implement the following policies and procedures:

1. User IDs or logon accounts can only be assigned with Department Head approval or by the assigned designee.
2. Department Heads or their designees are responsible for requesting the appropriate level of access and for staff to perform their job function.
3. All requests regarding user accounts or computer system access for workforce members are to be communicated to the system administrator. All requests shall be made using templates which will be made available on the County internal website in order to facilitate these and other requests. Any type of request for which a template has been made available must be made through that means
4. System administrators will only process requests that have been authorized by Department Heads or their designees through use of the appropriate template.
5. Using the appropriate templates for these requests creates the required electronic record of authorization, which is to be retained by the system administrator for a period of time the approved user has access, plus a minimum of one year.

Granting Access in an Emergency

Management has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if:

1. Management declares an emergency or is responding to a natural disaster that makes client information security secondary to personnel safety.
2. Management determines that granting immediate access is in the best interest of the client.
3. If emergency access is granted, the Department Heads or their designee shall review the impact of emergency access and document the event within 24 hours of it being granted.
4. After the emergency event is over, the user access shall be removed until the workforce member has completed the normal requirements for being granted access, requested by use of the appropriate template.

Termination or Suspension of Access

In the event of the following circumstances, Department Heads or their designees are responsible for making the necessary arrangements for removing a workforce member's access to EPHI and other sensitive and protected information. For access provided by the IT Department, they will use the appropriate template. If sensitive information is input and stored in third party/external/vendor programs or databases, they will follow those specific protocols for removing access to all.

1. If management has evidence or reason to believe the individual is using information systems or resources in a manner inconsistent with HIPAA Security Rule policies and/or

County policies as stated in these Wayne County IT Security and Confidentiality Policies.
2. If the workforce member or management has reason to believe the user's password has been compromised.
3. If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave.
4. If the workforce member's work role changes within the department and their system access requirements also change or if the member transfers to another department

If the workforce member is on a leave of absence and the user's system access will not be required for more than four weeks, management shall suspend the user's account until the workforce member returns from their leave of absence.

Modification to Access

If a workforce member changes their work role within the same department, the workforce member's Department Head or their designee is responsible for evaluating the member's current access and for requesting changes to their access to EPHI and other sensitive and protected information commensurate with the workforce member's new work role and responsibilities, by using the appropriate template. If a workforce member transfers to another department, their current Department Head or their designee will terminate user access, and their new Department Head or designee will request new access to EPHI or other sensitive and protected information, each using the appropriate template available on the County's internal website.

Ongoing Compliance for Access

In order to ensure that workforce members only have access to EPHI when it is required for their job function, the following actions shall be implemented:

1. Every new user ID or Log-On account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to the EPHI.
2. At least every six months, Information Technology (IT) teams are required to send managers or appropriate designees:
    - A list of workforce members for all applications
    - A list of all workforce members and their access rights for all shared folders that contain EPHI and other sensitive and protected information
    - A list of all workforce members approved for access to Virtual Private Network (VPN)
3. The managers or their designees shall then notify IT Support of any workforce members who no longer require access, using the appropriate template.

Department Head/Designee Responsibilities

1. Ensure that the access to EPHI and other sensitive and protected information granted to each of their workforce members is the minimum necessary access required for each such workforce member's work role and responsibilities.
2. In order to protect the security of the file server from malicious intent or unauthorized use by non-employees, each Department Head or an assigned designee is responsible to report employee termination (voluntary and non-voluntary), employee suspension, or employees expected to be on leave for more than four weeks (medical, worker's comp, etc.) to the IT Department minimally within 24 hours, using the appropriate form. In an urgent situation, immediate additional notification to the IT Department by phone be needed.
3. Request termination of access if the workforce member no longer requires access, using the appropriate form if access is provided by the IT Department. If sensitive information is input stored in third party/external/vendor programs or databases, they will follow those specific protocols for removing access to all.
4. Validate new User IDs or log-on accounts that are not used within 30 days of creation and provide IT with that information,
5. Review semi-annual user and folder access reports and the VPN access reports prepared by IT support and verify to determine if the workforce members still require access to EPHI.
6. Ensure that members of the workforce have signed the IT security agreement and are properly trained before approving access to EPHI and other sensitive and protected information.
7. Follow the appropriate security procedures when granting emergency access with support from IT where required.

IT Support Responsibilities

1. Immediately upon written notification, remove or modify a workforce member's access to EPHI and other sensitive and protected information for which the IT Department provides access.
2. Provide management with a report that identifies new User IDs or log-on accounts not used within 30 days of creation
3. Provide management with a semi-annual report documenting workers with access to EPHI, and requesting verification that access is still required to fulfill the worker's job functions.
4. When required, support management with the appropriate security procedures for granting emergency access.

Workforce member Responsibilities

Users of systems or applications that contain EPHI or other sensitive and protected information shall:

1. Verify by signing the appropriate forms that they have read both the Wayne County IT Security and Confidentiality Policies and the IT Security and Confidentiality Policy and

that they understand their responsibilities and the requirements they are to adhere to, and that they have received a copy of each.
2. Follow all Wayne County IT Security and Confidentiality Policies and requirements.
3. Complete HIPAA Privacy and Security training.
4. Immediately report all security incidents to their supervisor or other appropriate manner consistent with County Policy
5. Any employee who has a user account to access computer resources must take necessary precautions to keep confidential the passwords associated with that user account. Employees who feel that other individuals have knowledge of their password must change their password immediately.

Transmission Security

Purpose: The purpose of this policy is to guard against unauthorized access to, or modification of, electronic protected health information (EPHI) that is being transmitted over an electronic communications network. When EPHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.

General Policy:

Encryption

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose.

Encryption Required

1. No EPHI shall be sent outside the Wayne County Wide Area Network (WAN) unless it is encrypted. This includes all email and email attachments sent over the Internet.
2. When accessing a secure network an encryption communication method, such as a Virtual Private Network (VPN), shall be used.

Encryption Optional

1. When using a private circuit (point to point) to transmit EPHI, such as authorized transmission of EPHI within the Wayne County WAN, no encryption is required.
2. Dialup connections directly into secure networks are considered to be secure connections for EPHI and no encryption is required.

EPHI Transmissions Using Wireless LANs

1. The transmission of EPHI over a wireless network is permitted if both of the following conditions are met:

a. The connection through the wireless network utilizes an authentication mechanism to ensure that wireless devices connecting to the network are authorized
b. The connection through the wireless network utilizes an encryption mechanism for all transmissions over the network

2. If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI shall be encrypted before transmission.
3. Wireless devices are not to be connected to a wireless access point and to the Wayne County WAN at the same time. Wireless access capability must be disabled on any device that is connected to the Wayne County WAN.

Perimeter Security

1. Any external connection to the Wayne County WAN shall come through the perimeter security's managed point of entry.
2. If determined safe, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case by case basis.
4. All workforce members connecting to the Wayne County WAN shall sign the Wayne County IT Security Policy before connectivity is established.

Firewall Controls

1. Networks containing systems and applications with EPHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
   a. Limit network access to only authorized workforce members and entities
   b. Limit network access to only legitimate or established connections
   c. Console and other management ports shall be appropriately secured or disabled
3. The configuration of firewalls used to protect networks containing EPHI based systems and applications shall be IT department for review and approval.

Workforce Member Responsibilities

All workforce members that transmit EPHI outside the Wayne County WAN are responsible for ensuring the information is safeguarded by using encryption when using the Internet or a wireless connection.

IT Support Responsibilities

The Wayne County IT Department is responsible for the perimeter security architecture, its resources, its periodic auditing, and testing.

Workstation Security

Purpose: The purpose of this policy is to establish rules for securing workstations that access electronic protected health information (EPHI) as well has ones that have just general access. Since EPHI can be portable, this policy requires workforce members to protect EPHI at Wayne County worksites and all other locations.

General Policy: Wayne County shall implement safeguards to prevent unauthorized access to EPHI through workstations and to protect EPHI from any intentional or unintentional use or disclosure.

Workstation Security Controls

All workstations used by workforce members with access to EPHI shall be set to automatically lock the computer when it is left unattended, requiring the user to enter a password to unlock the workstation. The standard setting for the computer to lock after a period of inactivity is not to exceed 10 minutes. Workforce members shall manually lock their workstation computer using the Ctrl-Alt-Delete key combination when the computer is left unattended for any period of time.

Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens. At each site, every effort shall be made to ensure that confidential information on computer screens is not visible to unauthorized persons.

Workforce members who work from home or other non-office sites shall follow the above workstation security controls to safeguard EPHI access or viewing by any unauthorized individual.

Workforce members shall protect printed versions of EPHI that have been transmitted via fax or multi-use machines by promptly removing documents from shared devices.

Whenever possible, confidential documents are to be placed in locked cabinets or drawers when left unattended.

Department Head/Designee Responsivities

1. Control workforce member access to EPHI as per the User Access Management Policy.
2. Take appropriate corrective action if any workforce member knowingly violates the security of workstation use.
3. Ensure that all workforce members are locking their workstations when they are left unattended by using CTRL-ALT-DELETE then selecting Lock
4. Ensure that all confidential information is not viewable by unauthorized persons at workstations in offices under their management.

Workforce Member Responsibilities

1. Lock their computer when it is left unattended for any period of time.
2. Do not change or disable the automatic inability lock on their workstation.
3. Ensure that all confidential information in their workstation is not viewable or accessible by unauthorized persons.
4. When working from home or other non-office work sites, protect EPHI from unauthorized access or viewing.

IT Support Responsibilities

1. When installing new workstations, set the computer to automatically lock after the recommended period of inactivity, which is not to exceed 10 minutes.

Breach Notification

Purpose: The purpose of this policy is to formalize the response to, and reporting of, Personal or private information (PPI), Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII) data security or privacy breach or disclosure incidents. This includes identification and response to suspected or known privacy and security incidents, the mitigation of the harmful effects of known or suspected incidents to the extent possible, and the documentation of incidents and their outcomes. Note: while this policy was developed specifically to meet HIPAA regulations, the rules developed at Wayne County should always be applied to all protected information (see page 5 of this document): protected information should be interpreted as inclusive of all types of sensitive information, whether or not that is explicitly mentioned. This includes but is not limited to: Personal or private information (PPI), Protected Health Information (PHI), Electronic Protected Health Information (EPHI}, and Personally Identifiable Information (PII}, financial information AND electronic and hardcopy protected or private information.

General Policy: Wayne County will respond to all impermissible uses or disclosures of protected or private information and it will be presumed that a breach has occurred unless Wayne County or its business associate, as applicable, demonstrates through the appropriate risk assessment process, that there is a low probability that the protected or private information has been compromised. All disclosure, impermissible uses and breach incidents of electronic and hardcopy protected or private information shall be reported and responded to promptly.

Workforce member Responsibilities

Workforce members shall immediately notify their Department Head or assigned designee of any suspected or confirmed breach or disclosure incident. The Department Head or assigned designee shall report the incident to the County Compliance Officer at 315-946-5478. The

Compliance Officer will, in concert with the Security Officer and departmental Privacy Officers, evaluate the situation to determine the appropriate response to the report disclosure or breach incident, and initiate the response process as required by the type of incident.

Impermissible Uses, Breach or Disclosures Risk Assessment

The Compliance Officer, Privacy Officer, and Security Officer with the County Attorney will **WITHOUT UNREASONABLE DELAY**:

1. Perform and document a risk assessment based on the disclosure/breach identified: the process to be followed is - based on the current rule:
    a. Instead of assessing the risk of harm to the individual, Wayne County and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors:
        i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;(remember to include in the review a "sensitivity rating" - For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud - and if this is the case, then other laws may come into play);
        ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
        iii. Whether the protected health information was actually acquired or viewed; and
        iv. The extent to which the risk to the protected health information has been mitigated.

Impermissible Uses, Breach or Disclosures Response and Resolution

Wayne County, following a breach or suspected breach of unsecured protected health information or PII, shall:

1. Provide notice of a breach to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This notice is in

addition, not a substitute to, the required written notice, and shall be provided in the following form:

a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.
b. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.
c. Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
d. In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.
e. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of Wayne County's web site, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.
f. In any case deemed by Wayne County to require urgency because of possible imminent misuse of unsecured protected health information, Wayne County may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.
g. Inform prominent media outlets serving the State or jurisdiction.

2. Except as provided in §164.412, Wayne County shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
3. The content of the notification required shall meet the requirements of §164.404(c) and shall include to the extent possible:
    a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

c. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
d. A brief description of what Wayne County is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches;
e. Contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address; and
f. The notification shall be written in plain language.

Wayne County shall, following the discovery (post risk assessment) of a breach of unsecured protected health information as provided in §164.404(a)(2):

1. Notify the Secretary of HHS.
2. For breaches of unsecured protected health information involving 500 or more individuals, Wayne County will provide the notification required in the manner specified on the HHS web site located at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

3. For breaches of unsecured protected health information involving less than 500 individuals, Wayne County shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for those breaches occurring during the preceding calendar year, in a manner specified on the HHS web site at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Wayne County is required to notify all individuals when there has been or is reasonably believed to have been a unintended disclosure or compromise of the individual's private information (PII, PHR, PHI, etc.) in compliance with the applicable Information Security Breach and Notification Acts affecting Wayne County and this policy.

Impermissible Uses, Breach or Disclosures Response and Resolution Logging

Other than the above requirements for reporting to external agencies, all Impermissible Use, Breach, or Disclosure related incidents and their outcomes will be logged by the Compliance Officer and all findings, outcomes, and communications documented. That documentation will be saved for at least seven years or as needed to meet any claims, legal challenges, or other compliance activities.

Each calendar year, the log will be reviewed and disclosures will be reported to the Board of Supervisors by the Compliance Officer**.**

IT Asset Disposal

Purpose: The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Wayne County's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, cell phone's etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents. Therefore, all disposal procedures for retired IT assets must adhere to County approved methods.

Scope: This policy applies to the proper disposal of all non-leased Wayne County IT hardware, including but not limited to PCs, printers, handheld devices, servers, hubs, switches, bridges, routers and cell phones. County owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy. Where assets have not reached end of life, it is desirable to achieve some residual value of the IT asset in question through reassignment within a Wayne County department to a less-critical function.

Definitions:

- Non-leased refers to any and all IT assets that are the sole property of Wayne County; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.
- Disposal refers to recycling through responsible, ethical, and environmentally sound means or reassignment within a Wayne County department to a less-critical function.
- Obsolete refers to any and all equipment over 10 years old and/or that which no longer meets requisite functionality.
- Surplus refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.
- Beyond reasonable repair refers to any and all equipment whose condition requires fixing or refurbishing that is likely cost equal to or more than total replacement
- Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by Wayne County's IT department. The IT department is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills. The IT department is also responsible for acquiring credible documentation from third parties that are contracted to conduct the data wiping, tag or label removal, or any other part of the disposal process.

Acceptable methods for the disposal of IT assets are as follows:

- Reassigned to a less critical business operation function
- Recycled by a licensed and approved service provider in accordance with all local, state and federal laws, who by contract agrees to DOD wipe or to shred all data storage devices.

General Policy: It is the responsibility of Wayne County's IT department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of as described herein. To ensure the proper tracking of an asset and its correct status, the Information Technology department maintains an up-to-date asset inventory within the Help Desk

application (eHelpDesk). Every County IT related asset is included in this database with its current disposition status.

It is imperative that any disposals performed by Wayne County are done appropriately, responsibly, and ethically, as well as with County resource planning in mind. The disposal, sale or gifting of any County owned asset requires the written approval of the County Board of Supervisors in the form of an adopted resolution.

The following rules must therefore be observed:

- *Reassignment of Retired Assets*: Reassignment of computer hardware to a less-critical role is made at the sole discretion of the County's Information Technology department. It is, however, the goal of Wayne County to - whenever possible - reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.
- *Decommissioning of Assets*: All County surplus hardware slated for disposal by any means must be fully wiped clean of all County data or the hard drives must be destroyed. These must be certified destroyed or forensically wiped by the recycler and proof of destruction must be provided in writing.
- *Harmful Substances*: Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. The IT department may perform this action itself using government-approved disposal methods, or hire an accredited disposal County specializing in this service. No matter what the route taken, the removal and discarding of toxins from County equipment must be in full compliance with local and federal laws.

NYMIR Cyber Security Guide
Audit Trail:
A log should be maintained of all media that have been disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), sanitation or destruction method used, disposal method (such as sold or crushed).

Returning Media Under Warranty:
Many hard drives are purchased with a warranty period. When devices fail during the warranty period, the vendor normally requires the return of the defective drive before a warranty replacement is provided. Warranty return of a defective drive includes all the data, documents and information stored on the drive prior to the fatal problems. Since sensitive data could potentially be exposed on a warranty returned defective drive, the municipality should resort to physical destruction instead of returning the drive to the vendor. Your vendor may have an option to not return the hard drive.

IT Support Request – for problem Reporting/Trouble Calls

Purpose: This policy provides guidelines for Wayne County employees to place a support request or report an application or infrastructure problem with the Information Technology Department. All requests for access rights (including but not limited to user accounts, access to file shares or password protected applications) or for any other category for which a template has been provided on the internal website, should be directed to the IT department by the Department Head or an assigned designee, using the available appropriate template. Phone calls to the IT Department should be limited to large-scale issues which disrupt service for multiple users or interrupt a critical function, or to users who are at non-County locations or unable to use e-mail.

The goal of this procedure is:

To minimize disruption to the business, IT department and end users

To track and schedule IT changes

To track problems and the associated resolution

Scope: All support requests for problems with applications, networking or hardware should be entered into the Wayne County Help Desk application by sending an e-mail to ITsupport@co.wayne.ny.us. Departments may choose to direct their staff to have specific department members put in these requests on behalf of others. This policy applies to all local and remote employees, management, individuals such as Contractors, Consultants, Vendors, Interns, Research Partners, volunteers and other persons in similar positions, and any other parties who rely on access to Wayne County IT systems. While all approved moves, adds, and/or changes will be carried out in a timely a manner as possible, they may be delayed in the event of an IT-related problem or emergency.

General Policy: All Information Technology support requests for an application or infrastructure problem are to be entered into the IT Help Desk application by sending an e-mail to support@co.wayne.ny.us. Requests for access rights (including but not limited to user accounts, access to file shares or password protected applications) or for any other category for which a template has been provided on the internal website, should be directed to the Information Technology department using the available appropriate template by the Department Head or an assigned designee.

Media Copyright

Purpose: Wayne County has a responsibility in respecting and protecting the rights of intellectual property owners. This is not only a question of ethics, but also of law. Advances in electronic communication and technology, such as the Internet, have had a dramatic impact on

the way Wayne County conducts business, and have greatly facilitated our access to a wide range of information and media. As a result, the risk of copyright infringement, either intentional or accidental, is of increasing concern.

Scope: The goal of this policy is to inform information users at Wayne County of rules and procedures relating to copyright law compliance. This pertains to all County owned equipment and systems. It also pertains to any information posted on websites, social media sites, etc., by County employees as representatives of the County or if related in any way to their employment by the County, as well as to items in the list below (Copyrighted works). Information users include all County employees and individuals who work under the agreements with the County (such as Contractors, Consultants, Vendors, interns, volunteers and other persons in similar positions) to the extent of their present or past access to County information.

General Policy:

- Wayne County reserves the right to monitor end-user systems and the content stored therein. Wayne County also reserves the right to remove, delete, modify, or otherwise disable access to any materials found to be infringing on copyright.
- No employee of Wayne County may reproduce any copyrighted work in violation of the law. In the case of a County network, reproduction includes the replication of copyrighted works to the County's network.
- Copyrighted materials in the U.S. are not required by law to be registered, unlike patents and trademarks, and may not be required to carry the copyright symbol (©). Therefore, a copyrighted work may not be immediately recognizable. Information users should assume material is copyrighted until proven otherwise.
- If a work is copyrighted, the user must seek out and receive express written permission of the copyright holder to reproduce the copyrighted work in order to avoid violation.
- Copyrighted works include, but are not limited to: text (e.g. articles), images (e.g. photographs), graphics (e.g. logos), sound recordings (e.g. MP3s), video recordings (e.g. movies), or software programs. The following materials are not considered copyrighted materials: ideas, facts, processes, methods, systems, government works, and works in the public domain.

Medicaid Fraud Prevention

Purpose: The purpose of this policy is to protect Wayne County and its residents and maximize to the extent possible the revenue the County receives for providing healthcare services.

Scope: It is important that Wayne County regularly conduct a comprehensive screening of employees and vendors that provide healthcare services on the County's behalf. These employees and vendors will be matched against Federal and State databases that contain the name and identifying attributes of persons and organizations that are excluded from

participating in federally funded healthcare programs including, but not limited to, Medicaid, Medicare, and Child Health Plus.

General Policy: Wayne County will use software developed in-house, to monthly compare these employee and vendor names against federal and state databases that contain the name and identifying attributes of persons and organizations that are excluded from participating in a federally or state funded healthcare program including Medicaid, Medicare and Child Health Plus. This system will keep an audit of when the checks were done and the results of that comparison.
Situations in which employees or vendor names are matched against the downloaded federal and state databases must be resolved by the associated department head and the Compliance Committee. If an employee name and DOB is matched, the employee must be suspended until the 'excluded provider' information is resolved to the satisfaction of the Department Head. If the 'excluded provider' information is accurate and cannot be resolved, disciplinary action up to and including termination may occur.

Department Heads are responsible for ensuring employees have a current, active, valid license. Department Heads or their assigned designee are also responsible for timely updates to the list of their County employees and all individuals who work under agreements with the County (such as Contractors, Consultants, Vendors, interns, volunteers and other persons in similar positions) and have access to Protected Health Information and or Billable Services. A template to provide a means to report the necessary information (and changes) will be made available on the County internal website.

Online Banking

Purpose: There has been a significant increase in fraud involving the exploitation of valid online bank credentials. Despite on line banking establishments' security controls, there is no way to absolutely guarantee the safety of online banking. The tactics used to commit fraud can range dramatically in sophistication and continually evolve over time. Likewise, there is no single control that is most effective against cyber-attacks.

Scope: This policy applies to Wayne County systems that have access to on line bank accounts.

General Policy: Multiple layers of defense mechanisms will be utilized to protect the IT systems and information.

These include technology based:

- Up-to-date antivirus software
- Malware software

And non-technical controls:

- Only conducted from a wired rather than a wireless network
- Written agreement between Wayne County and the bank
- Bank has set dollar limits which requires a phone call from Treasurer's Office to override
- Limits on what accounts money can be transferred to is administered by the Treasurer's Office
- ACH File Transmittals require the bank file from IT as well as a "Schedule C ACH File Transmittal Form" from the Treasurer's Office which must match before processed
- Accounts are checked manually on a daily basis by the Treasurer's Office to be sure there are no unauthorized withdrawals.
- Department Heads and designees are responsible for training the users of these systems in proper procedures and protocols.

Remote Access

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for connecting to Wayne County's internal network from external hosts via remote access technology, and/or for utilizing the Internet for business purposes via third-party wireless Internet service providers (a.k.a. "hotspots"). Wayne County's resources (i.e. County data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all remote access and mobile privileges for County employees to enterprise resources – and for wireless Internet access via hotspots - must employ only County-approved methods.

Scope: This policy applies to all Wayne County employees and individuals who work under the agreements with the County (such as Contractors, Consultants, Vendors, interns, volunteers and other persons in similar positions) who utilize County- or personally-owned computers to remotely access the organization's data and networks. Employment at Wayne County does not automatically guarantee the granting of remote access privileges.

Any and all work performed for Wayne County on said computers by any and all employees as described above, through a remote access connection OF ANY KIND, is covered by this policy. Work can include (but is not limited to) e-mail correspondence, Web browsing, utilizing intranet resources, and any other County application used over the Internet. Remote access is defined as any connection to the County's network and/or other application from non-Wayne County networks, such as employee's home, a hotel room, airports, cafes, satellite office, wireless devices, etc.

All remote access will be centrally managed by the Wayne County Information Technology Department and will utilize encryption and strong authentication measures. Remote access connections covered by this policy include (but are not limited to) frame relays, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, etc.

Remote access will be requested by Department Heads or their assigned designees for their employees using a template which will be made available on the County Internal website. Access by contractors, vendors or others not directly employed by Wayne County will be through arrangement with the Director of Information Technology or an assigned representative of that department.

General Policy: It is the responsibility of any employee of Wayne County with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct Wayne County business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

- General access to the Internet by employees through the Wayne County network is permitted for business purposes only. Using this connection for any other purpose is prohibited.
- Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with the County's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All remote computer equipment and devices used for business interests, whether personal- or County-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Wayne County IT department.
- Remote users using public hotspots for wireless Internet access must employ for their devices a County-approved personal firewall, VPN, and any other security measure deemed necessary by the IT department. VP N's supplied by the wireless service provider should also be used, but only in conjunction with Wayne County's additional security measures.
- Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to Wayne County's network via remote access, with the obvious exception of Internet connectivity.
- If a personally- or County-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and Wayne County's IT department immediately.
- The remote access user also agrees to immediately report to their Department Head or assigned designee and the County's IT department any incident or suspected incident of unauthorized access and/or disclosure of County resources, databases, networks, etc.
- The remote access user also agrees to and accepts that his or her access and/or connection to Wayne County's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done to identify accounts/computers that may have been compromised by external parties.

Router/Switch Security

Purpose: This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Wayne County.

Scope: All routers and switches connected to Wayne County production networks are affected. Routers and switches within internal, secured labs are not affected.

General Policy:

Every router must meet the following configuration standards:

1. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
2. Disallow the following:
   a. IP (internet protocol) directed broadcasts
   b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
   c. TCP (transmission control protocol) small services
   d. UDP (user datagram protocol) small services
   e. All source routing
   f. All web services running on router
3. Use County standardized SNMP (simple network management protocol) community strings.
4. Access rules are to be added as business needs arise.
5. The router must be included in the County enterprise management system with a designated point of contact.
6. Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

Server Security

Purpose: The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Wayne County. Effective implementation of this policy will minimize unauthorized access to Wayne County proprietary information and technology.

Scope: This policy applies to server equipment owned and/or operated by Wayne County, and to servers registered under any Wayne County-owned internal network domain. This policy is specifically for equipment on the internal Wayne County network

General Policy:

Ownership and Responsibilities

All internal servers deployed at Wayne County are under the direct administration of the Information Technology Department which is responsible for all system administration.

General Configuration Guidelines

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of one week.
    - Daily incremental backups will be retained for at least one month
    - Monthly full backups will be retained for a minimum of 7 years.
- Security-related events will be reported to the IT Department, whose staff will review logs and report incidents to Information Systems management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks.
    - Evidence of unauthorized access to privileged accounts.
    - Anomalous occurrences that are not related to specific applications on the host.

Software Installation

Purpose: The purpose of this policy is to minimize the risk of loss of program functionality, the exposure of sensitive information contained within the Wayne County computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.
Scope: This policy covers all computers, servers, PDAs, smartphones, or other computing devices operating within Wayne County.

General Policy: Employees may not install software on Wayne County computing devices operated within the Wayne County network. Software requests must be approved by the requester's Department Head or their assigned designee via an available template on the internal website, or if that is not appropriate, send an e-mail to support@co.wayne.ny.us. Software must be selected from an approved software list maintained by the IT department, unless no selection on the list meets the requester's need. The IT department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Third Party Access

Purpose: To define the terms and conditions for remote connection to the Wayne County network by vendors, consultants or contractors. To protect Wayne County information from unauthorized access, use, and disclosure by providing guidelines for appropriate remote access.

Responsible Persons: Department heads or their designees who have contract authority with the third party are responsible for requesting for minimum necessary access for the third party.
Policy: Wayne County relies on the services of vendors and other third parties to complete many basic functions. Third parties pose security risks that exceed those of other users. Third parties, for example, may not benefit from security awareness training, background checks, remote office controls, and policy restrictions imposed on ordinary employees. Therefore, remote access privileges for vendors require special review and a high degree of trust with the vendor.

Eligibility: Remote access to Wayne County systems will only be granted to perform specific contracted functions. Third parties will be granted remote access into the Wayne County network only if they require it to perform maintenance, troubleshooting, upgrades, or monitoring for devices or systems they have provided to Wayne County. Access will be limited to the specific server(s) and communications ports (TCP/IP or UDP) which are the minimum necessary to perform the required support.

Granting Access: Vendors typically will request remote access during the technical review of their product or as part of the installation process. The Information Services Application Owner who is assigned to work with the vendor will provide the necessary information to the Information Security team to evaluate the vendor's requirements. The specific form of remote

access which is provided is determined by the Information Security team according to the business need and computing requirements for a given connection. Each request for vendor remote access will include specific system information (server names and communications ports), Wayne County contact information, and designation of a primary Point of Contact at the company.

Access: The preferred method of access is SSL/VPN/Citrix connection through the County's encrypted firewall using SSL client. The vendor will be provided RDP connectivity to resources as needed.

Confidential Data: Third parties may of necessity come in contact with Wayne County production systems containing Protected Health Information (PHI). All vendors must file a Business Associates Agreement (BAA) with the Wayne County Privacy Office before they can access Wayne County PHI. Third party staff may be required to complete Confidentiality and Non-Disclosure forms as a condition of access. All Wayne County vendors who access Wayne County systems are bound by the policy Acceptable Use. Access to Wayne County systems should never be granted to individuals who have not been authorized. Third party employees who work on site using County-provided network connectivity and/or computers are bound by the full set of Wayne County IT Security and Confidentiality Policies posted on the Wayne County site.

Protected information should be interpreted as inclusive of all types of sensitive information, whether or not that is explicitly mentioned. This includes but is not limited to: Personal or private information (PPI), Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII), financial information AND electronic and hardcopy protected or private information.

Security and Monitoring: All remote access sessions are subject to monitoring. At minimum, for each login the date, time, and username will be recorded. System records will also show the last time someone logged in and whether there were any access failures.

Termination of Remote Access: Upon termination of the contract, agreement or other official business arrangement with Wayne County, remote access will be terminated. In the case where individual credentials have been distributed, it is the Information Services Application Owner, who requested the access, responsibility to notify Wayne County IT to remove or disable that user's account. The Point of Contact will contact Wayne County IT when any new accounts or changes to existing accounts need to be made. A periodic review of all remote access users will be conducted to validate continued need for remote access. All unnecessary or unused remote access privileges will be terminated.

Video Security Surveillance

Purpose: The responsible use of video surveillance will tend to ensure safety and security of County property and premises, and all persons thereon, and assist in maintaining lawful and safe use of County premises.

Scope: This policy shall apply to all fixed video surveillance systems on County premises with the exception of such systems under the direct supervision of the Sheriff, systems under the direct supervision of the NYS Office of Court Administration, and with the further exception of covert systems employed by any law enforcement agency having jurisdiction.
General Policy: Video surveillance systems may only be deployed in public areas of County-controlled premises. Conspicuous signage will be posted in common areas to inform visitors, and employees that the area is being monitored.

No video surveillance system shall intentionally monitor private property except as necessary to adequately capture County premises. No recording video shall be viewed unless it is for system maintenance or is potentially material to a legitimate criminal or other governmental investigation. Recorded video shall not be released except as provided herein, or required by law.
Video developed under this policy may be monitored or copied only by law enforcement personnel authorized by the Sheriff or District Attorney, by the County Administrator, and by any other persons if authorized by a court of competent jurisdiction. If video includes a resident of the Wayne County Nursing Home, it can be released subject to HIPAA requirements. The Department of Information Technology may monitor, review, or copy only such video as may be necessary for system maintenance. A log of who accessed, when and for what purpose will be maintained by the Department of Information Technology.

Video developed under this policy shall be maintained at least 30 days after the date of recording, unless the Sheriff, District Attorney or County Administrator determines that specified video may be material and relevant to law enforcement or administrative investigation, or to potential litigation. In these cases, the imagery shall be destroyed or erased as soon as practicable, but no less than three years following the date of recording.

The Department of Information Technology shall be responsible for the operation and maintenance of the video surveillance systems covered by this policy.

Wireless Communication

Purpose: The purpose of this policy is to outline appropriate and inappropriate use of Wayne County's Wireless Networking resources, including

- Devices that are permitted to connect to the wireless network
- Standards for hardware and software that will be used
- Access privileges for the wireless network (i.e. who is authorized and who is not authorized to use the wireless network)
- Required security measures (including user passwords and how frequently they must be changed)
- Appropriate use of County assets (e.g. e-mail, Internet access)
- Consequences for violating the wireless networking policy.

Scope: Only County owned and approved wireless devices are permitted to connect to the wireless network. The Department of Information Technology is responsible for approving wireless devices for use on the network.

Non-County equipment will only be allowed to connect to designated wireless networks.

General Policy: The Department of Information Technology is responsible for setting standards for hardware, software, and other technology that will be used in the wireless network.

The Department of Information Technology is responsible for granting access privileges to the wireless network. To grant specific users access to the wireless network, their Department Head or assigned designee should use a template on the internal website, or if that is not available or suitable for the situation, send an e-mail to ITsupport@co.wayne.ny.us. This request should include specific users who need wireless networking access, the wireless devices they will use, the locations they will connect to the wireless network, and other information that the IT department may need.

All users accessing the wireless network must comply with County security policies. These policies include using network-access passwords, regularly changing these passwords, using encrypted connections, and other policies required by the IT department.

For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. Users are required to change their password if they have reason to believe that any unauthorized person has learned their password. Users are required to take all necessary precautions to prevent unauthorized access to Internet services.