INFORMATION TECHNOLOGY & INFORMATION SECURITY POLICY

Date of Adoption: April 10, 2019 **Policy#2019-0011**

Contents

Scope

The goal of information technology at Lenawee County is to provide a reliable and productive computing environment for Lenawee County staff, citizens and partners. The goal of this document is to set a standard regarding the confidentiality, integrity, availability, authentication, and nonrepudiation of Lenawee County's network infrastructure, and information technology assets. These Information Security Policies represent the efforts of the Lenawee County Information Technology Department (hereafter referred to as "Lenawee IT") to define a set of guidelines that provides a secure environment in which to manage and operate the County's information assets.

This policy will establish best practices and provide guidance for Lenawee County employees to follow in an effort to better secure our network infrastructure and IT assets. Standards and related processes and procedures will be developed and maintained to ensure compliance with these policies.

All departments and employees within Lenawee County will comply with the requirements and guidelines set forth in this policy, as well as any supporting documentation, designed to help facilitate the implementation of this policy. This policy is also intended to include compliance by any Lenawee County customer, vendor, contractor, or guest with a presence on, or device connected to, the Lenawee County network.

This policy applies to all Lenawee County employees, all businesses providing services to the County, customers/partners to which the County is providing services to, and governmental agencies which have the need to exchange communications or data information pertaining to Lenawee County business and services. Hereinafter this group will be identified as "staff, customers, and partners".

This policy also applies to all staff, customer, and partner use of County technology assets. County technology assets includes, but not limited to, desktop or laptop PCs, tablets, cell phones, smartphones, telecommunications systems, systems accessed remotely (webmail, Citrix, etc), servers, switches, and other network equipment.

Any agreements or contracts entered into between the County and its business service providers, customers, partners or governmental agreement/contracts shall not supersede these policies. Should any conflict occur between such agreements the order of interpretation are; these policies first and then any agreement or contract.

Adoption

The Information Technology and Information Security Policy **#2019-011** is **HEREBY** adopted by the Lenawee County Board of Commissioners at a regular meeting held Wednesday, April 10, 2019, in the Old County Courthouse, Adrian, Michigan.

Signed original on file with County Clerk

David Stimpson, Chair

Roxann Holloway, Clerk

Point of Contact

Contact the Lenawee IT Department helpdesk with any questions regarding this policy at (517) 264-4788.

Roles and Responsibilities

All users are responsible for:

- Knowing, understanding, and following all County policies.
- Exercising good judgment and acting in a professional manner when using County technology resources.
- Upon transfer to a new assignment, requesting that the authorities assigned to their User ID be changed to reflect the access requirements of the new job.
- Immediately reporting security incidents such as their computer becoming infected with a virus.

Management is responsible for:

- The actions of their staff, contractors, and volunteers and must ensure that all standards applicable to their environment are followed.
- Alerting Lenawee IT via the appropriate form, email, or the helpdesk line when a user transfers to new responsibilities. The privileges assigned to the user's ID must be changed to reflect the access requirements of the new job.

It is the responsibility of department heads and elected officials to ensure that County Information Security policies and procedures are followed by employees and others who may be under their direction within their departments.

It is the responsibility of county employees and others who use county equipment or facilities to adhere to all County Information Security policies and procedures.

All equipment, programs and services, provided to Lenawee County employees, customers, vendors and contractors, are solely for county government purposes. Individuals operating on such devices and connections should have no expectation of privacy. Such equipment and programs, and the files and communications contained thereon, are subject to review and removal at the discretion of the Lenawee County.

Technology, Internet, and Email Usage

These policies provide guidelines for the proper use of the Internet and email by Lenawee County employees and representatives of other organizations that access the County's Internet and email systems.

This policy applies to all Lenawee County employees, interns, contractors, vendors, temporaries and guests, including all personnel affiliated with third parties that have access to the Lenawee County network.

In part, this policy is established pursuant to the authority of the Enhanced Access Records Act, 1996 P.A. 462 and it does not amend or change any Lenawee County policy related to the Freedom of Information Act (FOIA).

Department heads and elected officials shall ensure that County Internet and email policies and procedures are followed by employees and others who may be under their direction.

Employee Conduct

At all times Lenawee County employees, interns, contractors, vendors, temporaries and guests, shall exercise good judgment and conduct themselves according to existing Lenawee County and individual department policies and procedures.

If it doesn't sound like a good idea, it probably isn't, ask your supervisor or Lenawee IT for clarification.

- While on work time the email systems and the Internet will be used for only Lenawee County business.
- Employees may use Internet access and email for personal use but these activities must be done on their own time. It is recommended that employees use personal email accounts for personal use in order to maintain a separation of work and personal activities. However, all access to the Internet and email using County equipment or facilities will be subject to the terms of this policy.
- Employees must use County email account(s) for County work.

Email Messages

All information contained within the email system is owned by Lenawee County and subject to the Freedom of Information Act. No confidentiality shall be assumed regardless of the content and nature of the message.

Web Sites and Web Content

It is the responsibility of department heads and elected officials to ensure that departmental web pages on the County websites are accurate and up to date and comply with County standards.

Lenawee County shall not allow advertisements, sponsorships or endorsements on County web sites, including vendor-hosted web sites. Links to businesses or other non-governmental organizations may be allowed when the link is strongly related to a County service.

The public shall not be required to provide personally identifiable information to visit Lenawee County's web site(s) to read or print information. County agencies may request personally identifiable information from the public in order to provide specific services that they request. Any information collected for that purpose shall be only that which is necessary to provide those services and will be handled as it would be on an in-person visit to a government office. Email addresses obtained as a result of a request to the County sites shall not be used for marketing purposes. Email or other information requests sent to the County web sites may be maintained in order to respond to the request or to forward the request to the appropriate department. Individuals may be able to receive updates on issues important to them but only if they choose that particular service. By choosing that service, they do not automatically choose other services. Should they subsequently choose not to receive such informational updates via email, they can remove themselves at any time.

In order to provide new services, design a more customer-friendly site and facilitate access to it, Lenawee County may conduct statistical analysis of the traffic on the site. Information that is not personally identifiable such as IP address, browser type and versions may be collected and used for this purpose. The site may not attempt to associate this data with information that is personally identifiable. Lenawee County shall not conduct or participate in on-line profiling (the practice of aggregating information about visitors' preferences and interests, gathered primarily by tracking their movements on line and using the resulting profiles to create targeted content on web sites).

Prohibited uses of the Internet and Email System

Prohibited uses of County equipment accessing Internet and email include, but are not limited to, the following, all of which shall be determined at the sole discretion of Lenawee County:

- Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed.
- Engaging in any form of intelligence collection from Lenawee County facilities.
- Unapproved political activities.
- Engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.
- Engaging in any activity that can be considered threatening, harassing, slanderous, or defamatory in nature.
- Any activities that will incur a cost to the County without prior authorization from a department head.
- Violation of copyright laws.

Internet Use by Elected Officials

Publicly funded access to the Internet by elected officials (and all County staff) will be utilized for activities related to County business and not for personal political use.

The following activities are prohibited for Lenawee County's elected officials when using County supplied Internet access and equipment:

- Soliciting funds for any candidate, ballot proposal, political party or political affiliate.
- Distributing/sending campaign materials or anything which a reasonable person would interpret as such.
- Distributing/sending appeals to vote for or against any candidate or ballot proposal.
- Illegal activities, threats, harassments, slander, defamation, obscene or suggestive messages or offensive graphical images, accessing pornographic materials, violation of copyright laws.

Social Media

Scope

This policy shall govern the use of social media by Lenawee County employees when posting for Lenawee County. Sharing information about County programs, news and activities through social media is an effective way to engage and inform the community. However, it needs to be done properly. If you use social media to post on behalf of Lenawee County, you must follow this policy. Social media sites shall include, but are not limited to: Facebook, Twitter, LinkedIn, Pinterest, Instagram and all other sites that are similar in content and/or character.

Seek Approval

You must have approval from your Department Head or his/her designee to use social media on behalf of the County. Once your Department Head or his/her designee has approved, you must contact the County's Information Technology Department to establish a social media account through the I.T. Service Center. I.T. must approve the social media site. Only social media sites approved by I.T. may be used on behalf of the County. The I.T. Department will retain password and log-in information for all County- sponsored social media. You must follow the I.T. standards for managing County- sponsored social media sites. To ensure the County has a consistent image on its social media sites, refer to I.T. standards for the look and feel of County-sponsored social media sites.

Respect County Resources

It is appropriate to use social media at work only when your use has been approved by your Department Head or his/her designee and is directly related to accomplishing work goals. You should participate in personal social media use on your own time. Personal social media use is use that has no official connection to your work at Lenawee County.

Be Accurate and Authentic

All County-sponsored social media sites must clearly identify that they are maintained by Lenawee County and prominently display County contact information. Your comments on such sites will directly reflect upon the County. Make sure posts are factually accurate. Cite and link to your sources where possible. If you make a mistake, admit it and correct it. When you post on behalf of the County you must identify your position with the County. Anonymous postings by County commentators are not allowed.

Be Aware of Legal Considerations

In order to avoid liability for yourself and the County, do not make comments that:

1) discriminate on the basis of race, creed, color, age, religion, sex, marital status, sexual orientation, national origin, weight, height or genetic information;
2) are sexual in nature;
3) compromise the safety or security of the County or individuals;
4) support or oppose a political candidate or ballot measure;
5) promote illegal activity;
6) violate another party's copyright, trademark or other protected property;
7) are obscene or profane.

Use good judgment when providing personal information and be aware of legal requirements and County/Department policies protecting a person's right to privacy. (e.g., HIPAA -- the Health Insurance Portability and Accountability Act protects a person's health information.) Ask for permission before posting someone's image, information, or intellectual property. Do not post information about employees, citizens, vendors, patients or clients being served by the County without first obtaining their written consent.

Retain posts

Because social media sites are not government sites, they do not follow the State of Michigan Record Retention Laws and Policies for Local Government. But social media conducted on behalf of the County is subject to these laws and policies and to the Michigan Freedom of Information Act. You must follow the State's record retention laws and policies[1].

1. More information about them can be found at the State of Michigan Department of Technology, Management and Budget website. http://www.michigan.gov/dmb/0,4568,7-150-9141_21738-96210--,00.html

Under the State's record retention rules, many of the items and documents you might post, such as notices of special events or holidays, and copies of documents already kept in your department do not need to be saved permanently. You must save a copy of these materials only until the event has passed, the case is closed, the project is completed, or the information has served its useful purpose. Most tweets and posts fall into this category because of their transient and temporary nature and because they do not perform a governmental function or create a County policy. However, you must also be prepared to respond to Freedom of Information Act requests or to produce documents and materials in a lawsuit. If you post something that is the only record of a County operation or is the only record that a County function has been performed, you must keep a copy.

Post Disclaimer and Removal

Prominently display the following statement on all sites that accept comments from the public:

"The County reserves the right to remove inappropriate comments including those that are discriminatory, obscene or sexual in nature, threaten or defame an individual or entity, support or oppose political candidates or proposals, violate the intellectual property rights of another party, promote illegal activity or commercial products or services or are not related to the topic in the original posting. Keep in mind that all of your posted comments are public records and subject to disclosure. Requests for public records may be submitted on the County website at www.lenawee.mi.us under the Freedom of Information section." Remove all posts that meet the criteria for removal stated above and keep a copy of the post.

Use of County Logos

Before using a County logo, you need to get the correct copy of the logo from the I.T. Department. Do not use a specialized logo, like the Sheriff's badge or other function specific logo unless you are posting on behalf of that department. You must use a County- owned logo exactly as produced by the I.T. Department. If you change the County logo, you could jeopardize the County's registration/ownership of the mark. If you want to make a significant change to a registered County logo, it must be approved by the Administrator's Office. If you display material that belongs to someone other than the County, you must give credit to the source or author of the material in your posting. Failure to cite a third party author or source could be a violation of federal law.

Compliance with County Policies

All County policies apply when you use social media on behalf of the County. This includes the **Communications Section** of this policy (use of County equipment for business purposes), **Equal Employment Opportunity Policy** (prohibits inappropriate conduct towards others because of their race, sex, age, etc.), **Harassment Policy** (prohibits inappropriate conduct or hostile work environment), and the **Personnel Handbook** (prohibits sharing of confidential information, profiting from County employment, prohibits political activities during work hours, in a County uniform, etc.). You may not use Social Media to advertise for private individuals, firms, or corporations, or imply in any manner that Lenawee County endorses or favors any specific commercial product, commodity, or service.

Personal Social Media

You may list your County position in your personal social media accounts but you are not authorized to speak or comment on behalf of the County. It is recommended that you keep your privacy and security in mind when engaging in personal social media use. Even with good security measures, the comments you make may be forwarded to others and accessible for others to see for a long time.

Violations

Employees found to have violated this policy may be subject to disciplinary action up to and including dismissal from employment pursuant to the County's Personnel Handbook or other applicable agreement, and, if applicable, may be subject to prosecution under federal or state laws.

Use of Collaborative Platforms

Lenawee County will endeavor to provide complete, secure and highly-available technology solutions for County departments. The County's ability to deliver services in-house may be outpaced by the capability of consumer and/or business-grade services that would be available for free or for-fee online. When business needs push the consideration of such services, the following considerations should be applied:

- When possible, County services should be used. If they cannot be used, the Lenawee IT will be notified prior to use.
- Online or cloud-based systems will be treated as an extension of the Lenawee County network infrastructure; as such all County policies will apply to the use of these systems.

Department heads will ensure that said documents have the correct permissions, and security settings.

Removable Storage Media and Offsite/Cloud Storage

Removable storage media includes but is not limited to, external hard drives, flash drives, and any device that will allow the user to remove files or documents from the Lenawee County network infrastructure. Offsite/Cloud Storage include services such as Google Docs, Box.com, DropBox or any other free or for-fee service can incur similar risks as removable storage media and must adhere to the same standards and policies as removable media. In addition if a department determines that these services are necessary, Lenawee IT must be notified prior to use.

- Documents classified as sensitive in nature should never be transferred off property via removable storage media. It is far too easy to accidentally misplace the device, thereby possibly creating a situation with legal ramifications.
- Users should scan their removable storage devices for malware before connecting it to any equipment within the Lenawee County network infrastructure.
- Lenawee IT reserves the right to monitor any device connected to the network infrastructure.

Ownership of File Systems and Storage

All electronic systems, hardware, software, temporary or permanent files and any related systems or devices, including all software, applications, or computer files created, written, or used by County employees on County time or by County employees on their own time using County equipment, shall be considered the property of the County.

Lenawee IT does not allow the storage of non-work-related files including, but not limited to, photographs, music, and movies on network storage devices, e.g. network drives G:, H:, M:, etc... Employees may use computers and telephones for limited personal use on their own time. Employees may not use equipment, such as printers, plotters or, network storage that consumes resources for personal use.

Right to Audit

Department heads or their designees and elected officials have the authority to inspect the contents of any equipment, files, voice mail messages, or other information in the normal course of their supervisory responsibilities. Reasons for reviews include, but are not limited to: system, hardware or software problems, general system failure, a lawsuit against the County, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is not available, or for any other work related reason as determined by the department head, elected official, or the County Administrator.

In accordance with approved procedures, Lenawee IT has the authority to access any equipment, files, voice mail messages, or other information in order to support the County's technology infrastructure. In doing so, Lenawee IT staff shall generally keep information confidential and may not violate County policy, state or federal regulations with respect to privacy and confidentiality in the course of their work and may not disclose the contents of such information to the public or staff.

The entry, utilization and distribution of data shall be in compliance with all applicable County, federal, and state regulations and statutes with regard to privacy and confidentiality.

Data and Information Handling

To ensure that information is handled responsibly, end-users must protect the data in their custody from inappropriate access, disclosure, or destruction. The degree of protection provided correlates directly with the sensitivity of data regardless of the media. The degree of protection afforded data must be consistent to help ensure all relevant laws, requirements and regulations are being met. Departments and/or programs may have data handling requirements that are different than County-wide guidelines. In such cases the more stringent requirement will prevail.

Transmission of Documents and Information Classified as Sensitive

The transmission of documents deemed as being of a sensitive nature, including but not limited to; ongoing court cases, Lenawee County Sheriff's department investigations, health information, or any information that individual departments would classify as sensitive is prohibited via any unsecured wireless access points. If you are uncertain if the documents or information should be considered sensitive, contact your department manager or Lenawee IT for guidance. Until you have received guidance, treat the documents as if they are considered sensitive in nature.

Data and Records Retention

Data which was initially collected and retained for normal business or legal purposes may no longer need to be retained. For this reason, all data and information must have a defined record retention period based on business requirements. Data may be retained beyond the guidelines specified only if it is necessary due to business requirements, outstanding Legal Hold, litigation, FOIA request, etc.

See Lenawee County's FOIA Policy

Be aware of record retention requirements of the State of Michigan available at https://www.michigan.gov/documents/dtmb/rms_Local_RM_Manual_640086_7.pdf

The Records Management Manual for Local Governments is prepared by the State of Michigan and all County Departments are to follow the most current schedule for proper record storage, retention, and destruction.

According to the manual, Michigan law requires that all records be listed on an approved Retention and Disposal Schedule that identifies how long the records must be kept, when they may be destroyed, and when certain records can be sent to the Archives of Michigan for permanent preservation. All Retention and Disposal Schedules must be formally approved by the Records Management Services (DTMB), the Archives of Michigan (DNRE) and the State Administrative Board.

Section 491 of the Penal Code (MCL 750.491) declares the improper disposal of local government records to be a crime.

The general schedules may be found online at: http://www.michigan.gov/recordsmanagement/

Email Retention

Employees shall retain email that has not fulfilled its legally mandated retention period by downloading and archiving the email in the appropriate departmental record retention media.

Departments shall ensure that its records are listed on an approved Records Retention and Disposal Schedule and shall ensure that all employees with email accounts are aware of and implement the policy.

Lenawee County Elected officials, Departments and Employees shall retain records under Departmental Records Retention unless otherwise directed by County Legal Counsel as it pertains to potential litigation or specific litigation hold.

Section 1. Introduction

Electronic mail (e-mail) is a means of exchanging messages and documents using telecommunications equipment and computers. A complete e-mail message not only includes the contents of the communication, but also the transactional information (dates and times that messages were sent, received, opened, deleted, etc.; as well as aliases and names of members of groups), and any attachments.

Section 2. Public Records

In accordance with the Michigan Freedom of Information Act (FOIA) (Public Act 442 of 1976, as amended), e-mail messages are public records if they are created or received as part of performing a public employee's official duties. All e-mail messages that are created, received or stored by a government agency are the property of the County of Lenawee. They are not the property of its employees, vendors or customers. E-mail accounts are provided to employees for conducting public business. Employees should have no expectation of privacy when using the agency's computer resources.

Section 3. Retention and Disposal Schedules

Michigan law requires that all public records be listed on an approved Retention and Disposal Schedule that identifies how long the records must be kept, when they may be destroyed and when certain records can be sent to the Archives of Michigan for permanent preservation. Retention and Disposal Schedules for local government agencies are approved by the Records Management Services, Archives of Michigan and the State Administrative Board. Records cannot be destroyed unless their disposal is authorized by an approved Retention and Disposal Schedule. The State of Michigan Records Management Services is available to advise local government agencies about a variety of records management issues.

Section 4. Retention Policy

Just like paper records, e-mail messages are used to support a variety of business processes. Just like paper records, senders and recipients of e-mail messages must evaluate each message to determine if they need to keep it as documentation of their role in a business process. Just like paper records, the retention period for an e-mail message is based upon its content and purpose, and it must be retained in accordance with the appropriate Retention and Disposal Schedule.

Section 5. E-Mail Storage and Maintenance

The County of Lenawee will retain its e-mail by printing e-mail and related transactional information, and filing the paper in a manual filing system.

Section 6. Employee Responsibilities

Employees are responsible for organizing their e-mail messages so they can be located and used. They are responsible for keeping e-mail messages for their entire retention period, and for disposing of e-mail messages in accordance with an approved Retention and Disposal Schedule.

Many agencies have established automatic purge routines for e-mail messages that are 30 or 60 days old. However, these purge routines are technology-driven and are not based upon Retention and Disposal Schedules. Many e-mail messages need to be retained longer than these periods of time. Employees are responsible for ensuring that e-mail messages with longer retention periods remain accessible until the

appropriate Retention and Disposal Schedule authorizes their destruction. *Note: Records, including e-mail, cannot be destroyed if they have been requested under FOIA, or if they are part of on-going litigation, even if their retention period has expired.*

Employees who use a home computer and a personal e-mail account to conduct government business must manage their work-related e-mail the same way as those messages that are created and received using government computer resources.

Just like paper records, e-mail messages might be subject to disclosure in accordance with FOIA. They can also be subject to discovery once litigation begins. Employees should be prepared to provide access to their e-mail to their FOIA Coordinator or an attorney for the County of Lenawee under these circumstances.

Section 7. Information Technology Staff Responsibilities

Individual employees are responsible for deleting messages in accordance with the appropriate Retention and Disposal Schedule. However, deleted messages may be stored on servers and backup tapes for several days, weeks or months after they are deleted. Information technology staff will ensure that deleted messages are rendered unrecoverable within 1 week of employee deletion. *Note: The destruction of e-mail messages on servers and backup tapes must cease when an agency becomes involved in litigation or when it receives a FOIA request.*

Many e-mail messages need to be kept longer than the original technology that was used to send and receive them. New technology is not always compatible with older technology that agencies may have used. Information technology staff will ensure that older e-mail messages remain accessible as technology is upgraded or changed. Each time technology upgrades and changes take place information technology staff will ask agency administrators for information about the existence and location of older messages so they can be migrated to the new technology.

Section 8. Administrator Responsibilities

Agency administrators are responsible for ensuring that their employees are aware of and implement this policy. They are also responsible for ensuring that their agency has an approved Retention and Disposal Schedule that covers all records (regardless of form or format) that are created and used by their employees.

Agency administrators are responsible for ensuring that the e-mail (and other records) of former employees are retained in accordance with approved Retention and Disposal Schedules.

Agency administrators are responsible for notifying information technology staff when the agency becomes involved in litigation or when a FOIA request that involves e-mail is received.

Section 9. FOIA Coordinator Responsibilities

Just like paper records, e-mail messages might be subject to disclosure in accordance with FOIA. FOIA coordinators are responsible for identifying if the records that are requested by the public are stored in e-mail, even if the public does not specifically request e-mail. They are also responsible for ensuring that information technology staff is notified that a FOIA requesting involving e-mail was received to prevent the destruction of relevant messages.

Section 10. Attorney Responsibilities

Just like paper records, e-mail messages might be subject to disclosure during the discovery phase of litigation. Attorneys representing Michigan government agencies are responsible for identifying if the records that are requested during the discovery process are stored in e-mail, even if the discovery order does not specifically request e-mail. They are also responsible for ensuring that information technology

staff is notified that a discovery order involving e-mail was received to prevent the destruction of relevant messages.

User Access

The purpose of this policy is to establish controls on the provisioning and revocation of access to County information systems and data and to enforce compliance with these Information Security Policies. Access to County resources will be formally controlled and granted only when a legitimate business need has been demonstrated and access has been approved to fulfill specific job requirements.

Access Control

Access to County information and information systems are controlled based on the concept of need-to know. Access will be granted, by departmental request, for an approved business and/or security function. Access must be revoked in a timely manner when that access is no longer required. Lenawee IT will establish and maintain Access Control standards and procedures necessary to control the provisioning or revocations of access rights to information systems and the data residing on those systems.

Access Reviews

Lenawee IT will establish Access Control standards and procedures which will include processes for conducting periodic access reviews. These reviews will be initiated by Lenawee IT and conducted by the County department managers and managers of partner and customer organizations to ensure that current access rights are appropriately provisioned. Any access deemed inappropriate during review will be revoked in a timely manner through the process defined by Lenawee IT.

Reporting Changes in Staff Responsibilities

Changes in employee position or responsibility frequently results in changes in "need to know" and therefore to system access privileges. It is the responsibility of the department head, elected official, or designee to report changes in staff assignments or job titles that would result in changes to access rights. Changes should be reported to Lenawee IT in a timely manner through the appropriate automated form or email so that access rights can be updated.

Passwords

Passwords are the "front line" of protection for any organization's information technology assets. Poorly chosen or compromised passwords can result in the compromise of Lenawee County's entire network.

These policies apply to passwords on all County devices or non-County devices connected to the County network such as, but not limited to, all computers either portable or stationary, tablets, cell phones, shared documents, cloud storage, Remote Access, Wireless Access, and Virtual Private Networks (VPN).

Password Length and Renewal

All passwords utilized by Lenawee County employees, vendors, contractors, or guests will meet a minimum length and utilize a combination of alpha-numeric and special characters as defined by the current FBI-CJIS/HIPAA standards. All passwords will be changed on a regular basis. Any individual who believes that their password may have been compromised must change it immediately and notify Lenawee IT through the Help Desk line.

Password Lock for Smartphones and Tablets

Smartphones and tablets connected to County systems are required to have a password lock.

Password Storage

Passwords, will not be written down, shared with anyone, or used for multiple accounts. Do not utilize the "Remember Password" feature in applications or web browsers. If anyone demands your password, refer them to this document, or Lenawee IT.

Password Protected Screen Saver

To help secure County owned physical devices or any device connected to the County network, a password protected screen saver is required to be activated after a predetermined time based on current FBI-CJIS/HIPAA standards.

Generic Accounts

In order to maintain non-repudiation in our network environment, the use of generic or shared accounts (domain accounts not assigned to an individual user) are prohibited. Non-Repudiation refers to the ability to know who does or did what on a computing system, or a service that provides proof of the integrity and origin of data, as well as an authentication that with high assurance can be asserted to be genuine. Any system, application, or database that currently uses a generic account will be required to develop a plan to remediate the issue. In the interim, it is required that the account owner documents the following:

- Name of the account, business purpose and a list of individuals with access to the account
- Method of monitoring account use and escalating when unauthorized use is detected
- Standard for regularly changing password

In no case shall an individual named user account be shared.

Remote Access

In order to promote efficiency and flexibility, Lenawee IT continues to develop means for employees, interns, contractors, vendors, and customers to access County systems both onsite and offsite and in some cases 24 hours per day. This policy applies to remote access connections used to do work on behalf of Lenawee County, including accessing applications, reading or sending email, and viewing intranet web resources.

This policy applies to all Lenawee County employees, interns, contractors, vendors and agents with a Lenawee County owned or personally-owned computer, laptop, workstation, tablet, cell phone, or any other device used to connect to the Lenawee County network. It is also applicable to connections made via remote servers, frame relays, ISDN, DSL, SSH, cable modems or other similar devices.

Remote Access General Policy

It is the responsibility of Lenawee County employees, interns, contractors, vendors and agents with remote access privileges to Lenawee County's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Lenawee County network.

Personal equipment that is used to connect to Lenawee County's networks must meet the requirements of Lenawee County owned equipment for remote access.

Remote access shall be used for business purposes only and the connection should be terminated (close connection or log off) when County business is complete.

Policies that apply to on premise access also apply to use of remote access.

Wireless Network Access

Lenawee IT continues to develop in-building wireless networking capabilities to increase staff and guest productivity and flexibility. The purpose of this section is to provide guidelines for access to wireless networks in general and access the Lenawee County internal network infrastructure via connections to wireless networks.

This policy applies to all Lenawee County staff, customers, and partners, including all personnel affiliated with third parties utilizing wireless technologies to access the Lenawee County network.

Wireless Access Policy

Lenawee County will establish separate wireless networks that provide a range of differentiated access and security. Lenawee IT will establish and publish Wireless Access Standards with current details on the configuration of wireless networks.

In general, secure wireless is only for County-managed devices to connect to the internal network. Public wireless is for devices that are not County-managed. Regardless of which wireless network the user has access to; end users must adhere to all standards and procedures defined by Lenawee IT for access and appropriate use.

Authorized Devices

The purpose of this policy is to identify which devices may be connected to the County's secure network and which will be treated as "guest" devices and therefore connected to a public network. This distinction is important to provide a higher level of reliability and security.

County-Managed and Non-County Managed Devices

A distinction is made between devices that are "County-managed" and those that are not. Only County-managed devices will have direct network login to the trusted County network. Devices that are County-managed include those that are provided by the County and are loaded with an Operating System image (e.g. Microsoft Windows) that has been developed by and is actively managed by Lenawee IT, including automated updates for the Operating System. Those devices that are not County-managed would be those that are commonly referred to as BYOD (Bring Your Own Device) systems. These could include user-owned laptops, smart phones or tablets that are not County managed. Regardless of the type of device or ownership, any device that is not County-managed will not be able to connect directly to the County private networks.

No device shall be added to the County's secure network without prior approval of Lenawee IT. Any unauthorized wireless device connected to the County secure network will be removed by Lenawee IT and the individual responsible shall be subject to rules of enforcement defined in this policy document.

Communications – Wireless, Pager, Phones, Faxes, Etc.

The Lenawee County wireless communications policy is to provide coordination of services and limited support for wireless devices used by Lenawee County employees who have a recognized business requirement and have the approval of their department head for the expenses involved.

Specific details are covered in the sections that follow. Wireless devices purchased with County funds shall be the "best fit" for the required situation. The best fit will be the most cost effective device that meets the documented need of the specific employee authorized by the department head to participate in the wireless program. An employee may purchase a more expensive device by prepaying the difference between the best fit option and the device of their choice. Wireless plans will be paid for out of department budgets based on the need determined by department heads. To use County funds

responsibly, County-sponsored wireless services are restricted based upon the type of service necessary to meet the individual user's responsibilities.

Vendors

In an effort to realize "economies of scale", the vendor selection will be submitted by the Information Technology department to the Administrators office for review and approval. Periodically a study will be conducted to certify a vendor in the following areas.

- County coverage
- State contracts
- Other negotiated co-op plans
- Price or costs
- Features
- Current needs

Wireless Plans

Information Technology responsibilities: To advise the Administrators office in tailoring wireless plans that first serve the County as a whole and then at the department level.

Department Head responsibilities: Determine and document the type of service needed based on the individual user's responsibilities. Obtain from the Information Technology Department the type and cost of the best fit device for each specific application.

Device use and protection

It is the responsibility of each employee to use reasonable care in handling and protecting wireless devices. In the event such equipment is lost, stolen, or damaged beyond repair, replacement costs shall follow the original purchase policy. If a pattern of neglect is identified the employee responsible for the device shall be responsible for the entire cost of replacement. Employees may, at the employee's expense, purchase insurance protection for their device.

Expenses above and beyond the wireless plan will be paid by the employee. Use of wireless devices while operating a motor vehicle is prohibited. Each department head is responsible for investigating abuse or misuse of any County resources.

Wireless device request process

An employee must submit a request to their department head for wireless products. Monthly fees for service will be paid for by the department in which the employee works. Best Fit wireless devices will be paid for from departmental funds. Prepaid funds for upgraded wireless devices shall be deposited in trust accounts and be distributed at time of purchase.

In the event of a staff termination/resignation

County-owned wireless devices must be turned in to their department head when the employee leaves the County. Any accessories provided with or for the device, or paid for by Lenawee County through the expense process, must also be turned in with the device. Upon separation from the County, the device and phone number may be released upon request and joint approval of the department head and the Information Technology Department.

Traditional paging services

Should an employee's job require a pager, the County will issue a pager according to the following guidelines:

- The cost of the device will be charged to the employee's department on a monthly basis.

- When the pager is issued, the employee will be given customer service information for the relevant paging company. Should the employee experience any difficulty with the pager, it is the employee's responsibility to contact the paging company to troubleshoot the difficulty.
- If the pager is lost, stolen, or damaged, the employee must notify their department head at once. The employee's department must pay for the cost of repair or replacement.
- If the employee's need for a pager should pass, or if other communication methods are adopted to replace the pager, the pager must be turned in to their department head.
- The pager must be turned in their department head upon moving to another department or leaving the County.

Telephone and Fax Communications

This policy is to provide services and limited support for telephones and fax machines to employees who have a recognized business requirement and have the approval of their department head for the expenses involved.

Specific details are covered in the sections that follow.

Device use

It is the responsibility of each employee to use reasonable care in handling and protecting telephone and fax devices provided by or paid for by the County. Should such equipment be lost, stolen, or damaged beyond repair, replacement costs must be borne by either the responsible employee or by the employee's department at the discretion of the employee's department head and depending upon the circumstances of the loss.

Telephone or Fax device request process

An employee must submit a request to their department head for telephone or fax products. Fees for the device will be paid for by the department in which the employee works.

Reporting phone loss, damage incident

Should an employee's telephone or fax be lost, stolen, or damaged beyond repair, the County will pay for a replacement only upon approval of the expense by the employee's department head. Costs for replacements will be billed to the employee's department.

All County Communication Devices/Equipment

As a matter of sound business practice, personal phone calls on County time and County phones are discouraged. Personal for-profit business is NOT ALLOWED on County owned equipment. Each department head is responsible for investigating abuse or misuse of any County resources; and may review the content of any County-owned communication equipment at any time.

Freedom of Information Act (FOIA)

In accordance with the Freedom of information Act, both county-owned and private communications equipment may be subject to FOIA requests.

Acquisition and Implementation of Technology Systems

This policy shall govern all technology purchases and implementations to ensure that they are made and used in accordance with the County's long term direction for technology. Additional detailed information regarding IT and telecommunication systems will be defined in associated procedures and standards.

Purchase of Technology Systems and Services

Lenawee IT shall create, maintain and administer standards and procedures for the purchase and use of computer and telecommunications systems, including, but not limited to: personal computers (PCs), printers, smart phones, tablets, scanners, telephones, Interactive Voice Recognition (IVR) Systems, Automated Call Distribution Systems (ACD), video and video conferencing.

All implementations of computer hardware, software, technology infrastructure, or telecommunications systems shall be in compliance with standards and compatible with the County's long-term direction for technology.

All purchases of computer hardware, software, technology infrastructure, or telecommunications systems shall be made by or with the approval of Lenawee IT and in accordance with the County's procurement procedures.

All grant applications that include computer hardware, software, technology infrastructure or telecommunications systems shall be reviewed and approved by Lenawee IT and a plan for replacement/maintenance shall be developed before they are submitted.

All devices connecting to the County's secured network including; computers, printers, tablets or other networked devices, must be approved and managed by Lenawee IT. Non-secured devices are not allowed to connect to the County's private network.

Unless otherwise mandated by state or federal regulations, all computer hardware, software, technology infrastructure or telecommunications systems shall be the property of Lenawee County and shall be under the control of the Board of Commissioners.

Software Licensing and Development

The Board of Commissioners acknowledges all pertinent license and copyright agreements affecting software. County employees are advised of their responsibility to abide by these agreements and are specifically forbidden to install or use software in a way that would violate the license agreement for the software. County employees are forbidden to copy or otherwise convert software in violation of copyright laws or license agreements.

All software, applications, or computer files created, written, or used by County employees on County time or by County employees on their own time using County equipment, shall be considered the property of the County.

Commitment to the Environment

Lenawee County is committed to minimizing the impact on the environment associated with purchase, use, and disposal of technology equipment. Lenawee IT will develop procedures and standards that reduce ongoing energy consumption and reduce the environmental impact of taking equipment out of service.

IT Systems and Network Operations

This policy applies to all information technology systems and assets owned and or operated by the County including but not limited to: Local Area Networks (LAN); Wide Area Networks (WAN), Virtual Private Networks (VPN) that connect users, partners, vendors and remote staff to County systems.

Administrator Accounts

Administrator accounts will be limited to the minimum number of staff required to perform those duties requiring elevated access. These accounts are to only be used for performing required administrative duties and not used for non-administrative functions. Individual end user accounts are to be used for daily employee business and not to be provided administrative privileges. Specified members of Lenawee IT based on their level of responsibility will be the only individuals assigned administrator accounts for the infrastructure, computers, switches, servers and other hardware equipment and such accounts will not be assigned to unapproved non-County IT staff.

Confidentiality

Lenawee IT staff and contractors in their normal course of work may come across sensitive information. Staff will hold such information in confidence, shall not share such information without authorization, shall not seek out confidential information, or use such information for personal gain. If, in the normal course of work, Lenawee IT staff comes across information that identifies or implicates illegal activity, he/she will report this information to the Administrator's Office. Additionally, if sensitive information is discovered that is not adequately safeguarded, staff will report to the Administrator's Office, department management and Lenawee IT so that corrective action can be taken. Lenawee IT will develop a non-disclosure agreement for staff and contractors to ensure understanding and compliance with this section of the Information Security Policies.

Patch Management (Operating System and Application Security Updates)

For County-managed devices, Lenawee IT will establish and maintain processes that will ensure all equipment has been updated with the latest updates prior to being placed into production as well as a process which defines how updates will be distributed to existing systems and applications. For non-county managed devices it is the user's responsibility to ensure that the devices being used to connect to the Lenawee County wireless network(s) have the most up-to-date security patches for the device's operating system, applications and peripheral devices.

Configuration Management

System hardening will be implemented for server, network and end user devices. Procedures will be developed and maintained that will, at a minimum, outline the following items:

- That only those components and software required to accomplish the specific business or IT purpose of the system or device will be installed.
- Standards that are consistent with best practices as recommend by vendors and industry sources will be followed.
- Ensure the removal of all vendor defaults such as guest or other generic accounts and their associated passwords from systems and applications.
- System security parameters that will be configured in a manner to prevent misuse.

Change Management

Lenawee IT will establish and maintain a formal change management process to ensure satisfactory control of all changes to equipment, software and related procedures. Change management procedures detailing the processes, roles, documentation and tools required to implement changes in the production environment will be documented and communicated to all existing and future Lenawee IT employees, interns, contractors and/or vendors as required.

Malware/Antivirus Protection

Lenawee IT will deploy anti-malware/anti-virus software on the network and end user systems in order to protect County systems from malicious code. Procedures for maintenance of anti-malware/anti-virus software will be documented and maintained by Lenawee IT.

Disaster Recovery and Business Continuity

The Office of Emergency Management and Lenawee IT shall develop, maintain, and administer a County-wide Disaster Recovery and Business Continuity Plan following industry best practices for such plans and be in compliance with federal and state regulations. The plan shall be reviewed, updated and tested on a regular basis. Included in the Disaster Recovery Plan will be a list of critical computer applications and the priority order, as determined by the County Administrator in which they will be restored to service in the event of a disaster that affects multiple applications. Each County department, in collaboration with Lenawee IT, will maintain their section of the business continuity plan to follow in the event of a disaster.

Lenawee IT will be responsible for backups of software and data on servers and network storage devices (not a local PC) under the management of that department. Backup copies of software and data shall be kept in a different physical location than the original versions.

Incident Response

Lenawee IT has deployed administrative, technical and physical controls to protect County IT assets and the information they contain. However, in the event a control fails to protect this information, Lenawee IT will establish and maintain an Incident Response process and procedure to mitigate the damage, investigate the cause, resolve the issue, and strengthen or implement new controls as needed.

Physical Access to IT Network Resources

Lenawee IT has the right to prohibit non-escorted staff, guests, vendor or contractors from entering locked rooms containing IT infrastructure equipment. Any access must be made through a request to Lenawee IT management.

Other Policy Compliance Requirements

Lenawee County is required to adhere to many external policies including but not limited to FBI-CJIS and HIPAA standards.

Annual Policy Review

This Information Security Policy will be reviewed on an annual basis or whenever there is a significant change to the County's IT Infrastructure or departmental structure that could impact the policy. Any changes will be documented, reviewed and submitted to the board of Commissioners for final approval.

Monitoring

The Lenawee IT reserves the right to monitor any device connected to the network infrastructure. All electronic systems, hardware, software, temporary or permanent files and any related systems or devices are the property of Lenawee County.

Lenawee IT, department heads or their designees and elected officials have the authority to inspect the contents of any equipment, files, and voicemail messages in the normal course of their supervisory responsibilities.

Reasons for reviews include, but are not limited to: system, hardware or software problems, general system failure, a lawsuit against the County, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is not available, or for any other work related reason as determined by the department head, elected officials, and the County Administrator.

Enforcement

Any employee, vendor, contractor or guest, found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or contract.

INFORMATION TECHNOLOGY & INFORMATION SECURITY POLICY

ACKNOWLEDGEMENT

I have read and understand the content and expectations of the Lenawee County Employee/Intern/Vendor/Contractor/Guest Information Security Policies Manual.

I acknowledge that I have access to a copy of this policy and agree to abide by the policy guidelines as a condition of my employment and my continuing employment, as a regular employee, a vendor, or a guest, with the Lenawee County Government.

I understand that if I have questions, at any time, regarding this acceptable use policy, I will consult with my immediate supervisor and/or Lenawee IT staff members.

Please read this policy carefully to ensure that you understand the policy before signing this document.

Employee Signature: _____

Employee Printed Name: _____

Date:_____

Glossary of Terms

Alpha-Numeric and Special Characters - For the purposes of this document, the term "Alpha-numeric and Special Characters" refers to, utilizing digits and punctuation characters as well as letters during passphrase creation e.g. A-Z, a-z, 0-9, !@#$%^&*()_+|~=\‘{}[]:";’<>?,./

Assets – For the purposes of this document, the term “assets” refers to, any electronic device connected to the Lenawee County network infrastructure.

Availability – For the purposes of this document, the term “Availability” refers to the last component of the CIA (Confidentiality, Integrity, Availability) Triad, and is one of the core principles of information security. In this context the term refers to the availability of Lenawee County data, systems, access channels, and authentication mechanisms.

Cable Modem - A device used to connect a single computer or a network to a cable company's service for Internet access. The same physical cable coming into the house or office also provides TV and voice (VoIP) service.

Cisco - Cisco Systems, Inc. is an American multinational corporation headquartered in San Jose, California, United States, that designs, manufactures, and sells networking equipment.

Confidentiality - For the purposes of this document, the term “Confidentiality” refers to the first component of the CIA (Confidentiality, Integrity, Availability) Triad, and is one of the core principles of information security. In this context the term refers to the confidentiality of Lenawee County data, systems, access channels, and authentication mechanisms.

DSL - Digital subscriber line is a family of technologies that provide internet access by transmitting digital data over the wires of a local telephone network.

Frame Relay - Refers to a standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology.

Hosts - Refers to any computing device that is connected to the Lenawee County network infrastructure.

Information Technology - Refers to the development, management, and use of computer-based information systems.

Integrity - For the purposes of this document, the term “Integrity”” refers to the second component of the CIA (Confidentiality, Integrity, and Availability) Triad, and is one of the core principles of information security. In this context the term refers to the integrity of Lenawee County data, systems, access channels, and authentication mechanisms.

ISDN - Integrated Services Digital Network (ISDN) is a set of communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.

Non- Repudiation – For the purposes of this document the term “Non- Repudiation” refers to, a service that provides proof of the integrity and origin of data, as well as an authentication that with high assurance can be asserted to be genuine.

Network Infrastructure - A Network's Infrastructure includes the physical hardware used to transmit data electronically such as routers, switches, gateways, bridges, and hubs.

Network Storage Device – any mass storage device connected to the County network (not local PC), primarily the County Data Center, commonly known to users as network drives: G:, H:, M:, etc…

Public/Private Keys - Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public.

Remote Access - Refers to a connection to a data-processing system from a remote location, for example through a virtual private network.

Security Patches or Security Updates- A security patch or security update is a change applied to an asset to correct the weakness described by a vulnerability.

Sensitive Information – Refers to any information that should not be within the public domain.

SSH - Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computing devices.

SSL / TLS- Refers to Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), these are cryptographic protocols that provide communication security over the Internet.

Virtual Private Network (VPN) - Refers to technology for using the Internet or another intermediate network to connect computing devices to isolated remote computer networks that would otherwise be inaccessible.

Wireless Network Access - Methodology that allows wireless devices to connect to a wired network using Wi-Fi, Bluetooth or related standards. Lenawee County has three (3) separate wireless network access points.