ELECTRONIC ACCEPTABLE USE POLICY

1. **PURPOSE:** Clinton County makes available and supports the use of technology for conducting business and performing job responsibilities. This Acceptable Use Policy lays out the acceptable uses of Clinton County's technological and informational assets for employee, contractor, consultant, temporary, and other party job responsibilities.

   The purpose of the Acceptable Use Policy is to notify all parties with access to Clinton County's information and/or information systems of their expected, acceptable, and restricted use. All employees (including permanent, temporary, full time and part-time staff, as well as commission-based staff) are required to review this policy as part of the employee handbook and annually attest that they have read, understand, and agree to adhere to its requirements. Third party service providers and like contractors with access to sensitive information and/or information systems are similarly bound through written contractual agreements and/or non-disclosure agreements.

2. **AUTHORITY:** The Clinton County Board of Commissioners.

3. **APPLICATION:** This policy applies to all County Elected Officials, Department Heads and Employees, Interns and Volunteers.

4. **RESPONSIBILITY:** The County Administrator and/or designee shall be responsible for implementation of this policy.

5. **DEFINITIONS:**

   5.1. E-mail: acronym for electronic mail.

   5.2. Electronic Communications: All communications and information transmitted by, received from, entered onto, or stored on county owned technology resources, including but not limited to e-mail, cell phone calls, GPS locations, voice mail, texting, and instant messaging.

   5.3. Internet: The Internet is a worldwide "network of networks" including bulletin boards, WWW; World Wide Web servers, applications, messaging services and other functions and features which can be accessed via a computer, a Smartphone or other client device.

   5.4. County owned technology resources: Technology resources paid for by county funds, including but not limited to: internet/intranet, computer equipment (desktops, laptops, printers), telephones, smartphones, software, operating systems, storage media, network accounts providing electronic mail, and systems that enable web browsing and file transfer.

5.5. Malware: a general term for potentially hostile software; encompasses viruses, Trojans, spyware, etc.

5.6. Data Classification: Confidential information including constituent and sensitive county data requires appropriate protection. Safeguarding this information is required of all employees. All information is categorized as follows:

5.6.1. Public – Can be shared without concern.
5.6.2. Operational – Used inside the County.
5.6.3. Regulated – There are regulations addressing the data.
5.6.4. Business Critical – The data is of vital importance.

6. POLICY:

6.1. **OWNERSHIP:** All county owned technology resources are the property of Clinton County. All electronic communications are the property of Clinton County. Electronic communications may be subject to Freedom of Information Act (FOIA) requests and other legal disclosure.

6.1.1. All equipment and applications on county owned technology resources must be authorized and installed by appropriate personnel. Only software and hardware communication protocols that meet the County's defined standards will be installed unless an exception has been documented in writing.

6.1.2. The County reserves the right to access, inspect or remove any county owned technology resources provided or used by any individual.

6.2. **GENERAL INSTRUCTIONS FOR COUNTY EMPLOYEES REGARDING THE USE OF COUNTY OWNED TECHNOLOGY RESOURCES:** County employees will not access constituent confidential information unless this access is needed in the performance of assigned duties. We must recognize, however, that while performing county duties, county employees of necessity acquire confidential information considered to be extremely sensitive by constituents. This information must not be revealed to unauthorized persons. In addition, this information should not be discussed with others within the county unless their duties also require the information. Constituent financial information can be released only when authorized by the constituent, when ordered by a court or the Internal Revenue Service (IRS), or in response to a properly authorized Freedom of Information Act request. Any such information released must be accurate and within the confines of the authorizing document. In all cases the release of constituent information will be based on a written request.

Clinton County takes reasonable steps to maintain the secrecy of such information and it is to remain confidential, both while you are a Clinton County employee, and afterward if your employment should end. You are bound not to use or disclose any such

information after your employment ends, or during your employment, except as necessary while performing job duties.

When using county owned technology resources, take care to ensure that all communications and messages are courteous, professional, and businesslike. Remember that the quality and content of your communications is a reflection on the County. Employees are responsible for exercising good judgment regarding the reasonableness of their use of county owned technology resources. If there is any uncertainty, you should consult the County IT Department.

6.3. **USAGE OF COUNTY OWNED TECHNOLOGY RESOURCES:** County owned technology resources are an asset of our County and are protected from unauthorized access, disclosure, modification, and destruction, whether accidental or intentional. It is our policy that all county employees will use county owned technology resources provided to them for county purposes.

Clinton County uses computer software in its daily operations. In most cases, Clinton County does not own the software but is only licensed to use it. Any duplication of software, except for backup purposes, violates both the license agreements and the copyright laws, and could subject the County and the individual to civil damages and criminal penalties that include fines and imprisonment. No individual may copy software or its accompanying documentation for use on any other computer at the County or elsewhere. Employees may not give the county software or copies of the county's software to anyone without prior management approval.

6.4. **USERS:** Only Clinton County employees and elected officials (interns in some circumstances authorized by their supervisor) who have county e-mail accounts and passwords are permitted to use these systems. County e-mail accounts will only be established once the employee has read Clinton County's Electronic Acceptable Use Policy, has signed the Acknowledgement Form, and received their supervisor's signed authorization. Upon termination of employment (or separation when applicable to interns and volunteers), that user's county e-mail account and privileges will be revoked.

6.4.1. Vendors that are providers of the various software programs utilized by the County occasionally need access to the respective server housing their programs. This access is necessary for upgrades, program "fixes" and other support needs. This remote vendor access will only be allowed through the County's Virtual Private Network (VPN) and initiated by IT Department staff.

6.5. **ACCEPTABLE ACTIVITIES:** The use of county owned technology resources is a fundamental part of successful daily operations. To ensure Clinton County can operate

successfully, employees may use county owned technology resources for the following activities:

6.5.1. Use of county owned technology resources to complete the activities specified in their job descriptions.

6.5.2. Use of electronic communication to communicate with constituents and other employees to meet operational needs.

6.5.3. Accessing systems and resources, which they have been authorized to use.

6.5.4. Accessing approved online resources.

6.6. **PROHIBITED USES:** Under no circumstances is an employee of Clinton County authorized to use county owned technology resources to engage in any activity that is illegal under local, state, federal or international law. It is expected that employees keep in mind that access to county owned technology resources is for public purposes. Use of the internet is subject to all other county policies. In addition, the list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use of county owned technology resources.

At no time, unless directly authorized by management, shall a party attempt to bypass any security control or access information for which they do not have sufficient privileges. Additionally, at no time is any party authorized to perform any of the following actions using county owned technology resources:

6.6.1. Using county owned technology resources in any way that intentionally or unintentionally violates any applicable local, state, national, or international law or any rules or regulations published under the terms or authority of such laws.

6.6.2. Using county owned technology resources in a way that violates intellectual property (copyright, trademark, patent, or trade secret) laws. Infringement does not have to be deliberate to be actionable.

6.6.3. Using county owned technology resources to circumvent the Open Meetings Act.

6.6.4. Downloading of non-business-related data (including, but not limited to music, personal pictures, and video).

6.6.5. Downloading of non-approved applications programs.

6.6.6. Misrepresenting one's identity for any purpose, including composing or intercepting messages, except for approved undercover investigations or other authorized “send on behalf of” identities.

6.6.7. Revealing your e-mail access code or password to another employee (there may be exceptions, so obtaining written permission is advisable.)

6.6.8. Using county owned technology resources for commercial purposes other than the business of Clinton County.

6.6.9. Using county owned technology resources to communicate prejudice or otherwise create a hostile work environment.

6.6.10. Unauthorized use of county owned technology resources for purposes of lobbying, or for solicitation.

6.6.11. Creating offensive, disruptive, or malicious messages. These include, but are not limited to messages which contain profanity, sexually explicit content, race, national origin or gender specific comments, threats, or harassment.

6.6.12. Viewing, accessing, uploading, downloading, storing, transmitting, or otherwise manipulate pornographic or other sexually explicit materials is prohibited.

6.6.13. Using county owned technology resources for religious or political activities or other similar purposes.

6.6.14. Using county owned technology resources for gambling, betting pools or investment clubs.

6.6.15. Job hunting.

6.6.16. Engaging in any activity that would create liability for Clinton County.

6.6.17. Any attempt, including the use of proxy sites, to bypass the County's internet filtering system is prohibited.

6.6.18. Sharing or storing unlicensed software or audio/video files.

6.6.19. Using security exploit tools (hacking tools) to attempt to elevate user privileges or obtain unauthorized resources; broadcasting e-mail to large numbers of the public or employees (SPAM).

6.6.20. Using a county e-mail address(es) and/or county owned technology resources when posting to public forums e.g., blogs, social media sites, wikis, and discussion lists for personal use.

6.6.21. Accessing sites that distribute computer security exploits ("hacking" sites).

6.6.22. Using county owned technology resources to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters."

6.6.23. Making fraudulent offers of products, items, or services originating from any Clinton County account.

6.6.24. Using county owned technology resources to access (or to attempt to access) the accounts of others, or sniff network traffic, or to penetrate (or attempt to penetrate) security measures of Clinton County's or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data.

6.6.25. Using county owned technology resources for any activity which adversely affects the ability of other people or systems to use county owned technology resources. This includes a Distributed Denial of Service (DDoS) attack, spreading malicious software, and excessive use of computing or network resources.

6.6.26. Visiting unapproved websites or website content that is not directly related to job responsibilities. Unapproved website content includes, but is not limited to nudism, pornography, adult mature content, violence, racism, hate, sex education, gambling, or illegal/questionable skills.

6.6.27. Introducing any unapproved CD's, floppy disks, USB devices, wireless gateways, routers, switches, or other media/hardware to any Clinton County system without first engaging the IT Director for approval.

6.6.28. Opening unknown attachments to electronic mail. Users should never, under any circumstances, open email attachments from unknown parties or those of a suspicious nature.

6.6.29. Using county owned technology resources to transmit unencrypted, internal, or confidential information or files that are not for county use or for malicious purposes.

6.6.30. Using electronic communications that include any private and/or confidential material. All county controls and regulatory requirements for written or oral communications also apply to electronic communications.

6.6.31. Email messages received from unknown parties should not be opened and should be immediately deleted from both the inbox and deleted items folders.

6.6.32. Personal email, texting, instant messaging, or other personal electronic communication should never be utilized for official County business unless approved in advance by the IT Director and the appropriate manager.

6.6.33. Email distribution should be carefully considered; before copying to others a message directed to a specific employee, the type of information and question of confidentiality should be carefully considered.

6.6.34. Utilize the County's secure email solution when the requirement to send or receive nonpublic constituent information arises.

6.6.35. Revealing or publicizing confidential or proprietary information which includes, but is not limited to account passwords, financial information, confidential constituent information, databases and any information contained therein, computer/network access codes, and business relationships.

6.6.36. Copying software or media, for any reason, that has been purchased, developed, or is owned or licensed by the County, without prior authorization.

6.6.37. Altering the county network infrastructure without prior authorization and proper instruction. The network infrastructure consists of, and is not limited to workstations, servers, wiring, switches, hubs, routers, firewalls, wireless devices, modems, internet connections, phone lines, and power connections.

6.6.38. Altering or disabling malicious software protection programs is strictly prohibited unless prior authorization is received. Users are also required to report any suspicious or actual malicious software activity immediately to the IT Director.

6.6.39. Use of any cloud storage or file sharing services that are not formally approved by the IT Director and/or county approved. This includes but is not limited to

Dropbox, Amazon, Google Drive, Box, One Drive, Sync, pCloud, Carbonite, Crashplan, iDrive, iCloud, Elephant Drive, JottaCloud, BackBlaze, SugarSync, Egnyte, Backupvault, and Sharefile.

6.6.40. Use of any electronic equipment not owned by the County to access the VPN is prohibited unless approved in advance by the IT Director and the appropriate manager.

6.7. **PERSONAL USE:** Clinton County understands that incidental and occasional use of county owned technology resources for personal communications will happen. Individuals should understand that they should have no expectation of privacy in connection with the use of county owned technology resources. This limited personal use shall incur no cost to the County, not interfere with work responsibilities, nor disrupt the workplace.

6.7.1. County owned technology resources shall not be used to store personal items, including but not limited to images (photos), videos, music or personal communications or documents.

6.8. **MOBILE DEVICE USAGE:** This section applies to county provided mobile devices and personal mobile devices. Mobile devices used for county purposes must be approved for use by management prior to connecting them to the information systems of the County. The addition of new hardware, software, and/or related components to provide additional mobile device related connectivity within county facilities will be managed by the Clinton County IT Department. Non-sanctioned installations of mobile device related hardware, software, and/or related components, or use of same is strictly forbidden. All hardware security configurations must be approved by the Clinton County IT Department. When using mobile devices, the employee will comply with the following guidelines.

GENERAL USER RESPONSIBILITIES:

6.8.1. Employees shall limit the use of personal mobile devices during business hours. Employees are permitted to utilize personal mobile devices either before or after the business hours or during breaks or meal periods. Additionally, Clinton County shall not permit employees to connect personal mobile devices to Clinton County networks, wired or wireless unless authorized by management.

6.8.2. Employees should refrain from using their personal mobile devices for county purposes unless authorized.

6.8.3. Using cellular phone cameras to electronically transmit images of confidential constituent or county information, or images of employee or constituents, is prohibited unless managerial approval is acquired.

6.8.4. Using online or mass storage devices such as external hard drives, thumb drives, iCloud, Google Drive, SkyDrive, Mozy, SugarSync, Dropbox or the like in

conjunction with mass amounts of non-public constituent information is prohibited unless prior approval is given by the IT Director.

6.8.5. Users accessing the County's wireless network also agree to and accept that their access and/or connection to Clinton County's network may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity.

USER RESPONSIBILITIES FOR COUNTY USE:

6.8.6. All county owned mobile devices are to be used primarily for county use.

6.8.7. Although IT is not able to manage the public network to which mobile devices initially connect, users are expected to adhere to the same security protocols while utilizing this equipment.

6.8.8. All other sections of the Clinton County Electronics Acceptable Use Policy apply to mobile devices as well.

6.8.9. Users are expected to physically secure all mobile devices, whether personally owned or issued by Clinton County if they are used for county purposes and/or have access to Clinton County information resources.

6.8.10. The mobile device user agrees to immediately notify the Clinton County IT Department or IT Director if they suspect their mobile device has been tampered with, accessed by an unauthorized person, lost, or stolen. Immediate action in these situations has a direct impact on the potential damages incurred by the County.

6.8.11. Employees are prohibited from using their phone while driving. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call. If acceptance of a call is unavoidable and pulling over is not an option, employees are expected to keep the call short, use hands-free options if available, refrain from complicated or emotional discussions, and keep their eyes on the road. Special care should be taken in situations where there is traffic, inclement weather, or the employee is driving in an unfamiliar area.

6.8.12. Clinton County reserves the right to turn off without notice any access port to the network that puts the County's systems, data, users, and constituents at risk.

6.8.13. If a county owned mobile device is damaged and cannot be appropriately wiped of data and verified as secure, the device will be physically destroyed, and replacement will be at the discretion and approval of management.

6.8.14. County data stored on the personal or county provided mobile device is owned by Clinton County and is not for distribution outside of the county. Willful mishandling, loss, theft or destruction of county data or equipment will not be tolerated and the employee at fault may be subject to dismissal and criminal charges.

6.8.15. Clinton County is not responsible for any personal information which includes, but is not limited to pictures, music and apps stored on a county owned mobile

device. Clinton County IT Department will not be responsible for restoring any personal information on the mobile device in the event of a failed or lost device.

6.8.16. Clinton County reserves the right to block and/or delete any application installed on a county owned mobile device at any time. Users are responsible for their own app purchases. Clinton County will not buy or reimburse any charges for applications and/or usage. Application usage will be monitored and reviewed on a regular basis.

6.8.17. Users of county owned mobile devices are expected to use internet services within reasonable limits.

6.8.18. Users traveling outside of the US should contact IT at least 14 days prior to ensure their mobile devices will work properly while traveling abroad. Prior management approval is required for this type of change in temporary access.

6.8.19. Guard against inadvertently disclosing non-public information while using a mobile device. Privacy and confidentiality need to remain top of mind when using mobile devices outside of county premises and in the public.

6.8.20. Text messaging (as per Michigan Law) is not allowed while driving. Under no circumstances are employees allowed to place themselves or others at risk to fulfill county needs. Employees who are charged with traffic violations resulting from the use of their phone while driving will be solely responsible for all liabilities that result from such action.

6.8.21. Updating the device operating system and applications is the device user's responsibility. Clinton County reserves the right to enforce adherence to specific patch levels and decline access to county data and network resources until those specific patch levels are met.

6.9. **MONITORING/PRIVACY**: Clinton County reserves the right to access, monitor, and disclose (with or without notice) any use of county owned technology resources, including but not limited to any electronic communications made via the internet, e-mail, telephone, or any electronically stored information. Individuals shall have no expectation of privacy for any electronic communication made, received, transmitted or stored on county owned technology resources. It is possible that unencrypted electronic communications sent from county owned technology resources can be intercepted on the system and on the internet; therefore, the user should not expect any degree of privacy in the use of county owned technology resources. E-mail messages deleted by the user may be retrievable from the hard drive, backup tapes, or the receiving or sending e-mail system.

6.9.1. County owned technology resources shall not be used to store personal items including but not limited to images (photos), videos, music or personal communications or documents.

6.9.2. Clinton County utilizes software which can limit access to certain websites. In addition, this software allows the tracking of websites visited and the amount of time spent on a particular site.

6.10. **IDENTIFICATION OF COUNTY RESOURCES:** The use of county resources shall be clearly indicated in all communications utilizing the internet or e-mail services.

6.10.1. Each e-mail message shall include a signature line. At a minimum the signature shall include the name, department, mailing address and telephone number of the user. At the bottom of the signature block, every message will prominently state *"This message has been prepared on resources owned by Clinton County, Michigan. It is subject to the Electronic Acceptable Use Policy of Clinton County."*

6.11. **REMOTE ACCESS:** An authorized employee may access a county account from a remote location other than the site designated for that account (e.g., telecommuting or checking e-mail while away from the office on business). To obtain authorization, individuals seeking remote access must review and agree to the Remote Work Agreement in Appendix A.

REMOTE ACCESS OVERVIEW:

6.11.1. All Clinton County employees, elected officials, interns, and volunteers who have been authorized to utilize mobile devices such as Smartphones or laptop computers that synchronizes information with county resources (including email) are responsible for securing their device to prevent sensitive data from being lost or compromised, viruses being spread, and other forms of abuse. It is required that all Smartphone devices be password protected. You will be required to know what that password is and to not distribute to anyone. If a web or email enabled phone or personal digital assistant (PDA) device is lost, stolen, or believed to be compromised, the incident should be reported to IT immediately.

6.11.2. Authorized employees may use privately owned connections for county purposes. If this is the case the employee is responsible for all costs associated with that connection. In addition, the County's IT Department cannot and will not technically support a third-party internet service provider (ISP) connection or hotspot wireless ISP connection.

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

6.11.4. Users of Smartphones and other wireless devices that use public or commercial access sites (Wi-Fi hot spots, cellular towers, etc.) need to bear in mind that sensitive information should not be transmitted via any offsite access points unless such communications are encrypted in both directions.

6.11.5. When accessing the Clinton County network from a personal device, authorized users are responsible for preventing access to any Clinton County computer resources or data by non-authorized users. Performance of illegal activities through the Clinton County network by any user (authorized or otherwise) is prohibited. The authorized user bears responsibility for and consequences of misuse of the authorized user's access.

REMOTE SECURITY REQUIREMENTS:

6.11.6. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs), TLS, Etc.), strong passwords and multi-factor authentication (i.e., Soft or Hard Tokens).

6.11.7. Authorized users shall protect their login, password, and tokens, even from family members.

6.11.8. While using a Clinton County-owned or personal device to remotely connect to Clinton County's network, authorized users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized user or third party.

6.11.9. Use of external resources to conduct Clinton County business must be approved in advance by IT Director and the appropriate manager.

6.11.10. All hosts that are connected to Clinton County internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

6.11.11. Authorized users agree to abide by this Acceptable Use Policy in its entirety while performing work related functions remotely.

6.11.12. Authorized users agree to immediately report to their manager, Clinton County's IT department, and IT Director of any incident or suspected incidents of unauthorized access and/or disclosure of county resources, databases, networks, etc.

6.11.13. Authorized users agree to and accept that their access and/or connection to Clinton 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 in order to identify accounts/computers that may have been compromised by external parties.

6.12. **USERNAME AND PASSWORD RESPONSIBILITIES:** Users shall never share their usernames and passwords with anyone for any reason and will be held accountable for any actions taken with their credentials. Not all systems can meet the same password requirements and therefore users of these systems must construct the strongest possible password allowable by the system and will be held accountable for failing to meet password standards. Use of a Passphrase is strongly encouraged versus a password when possible. Passphrases are longer than 14 characters and keyed in like a sentence. They are

easier to remember and much more difficult to crack. Passwords are an integral part of the County's security program. As such the following guidelines have been established:

6.12.1. If the system allows, or unless approved by management, password should be at least 14 characters in length.
6.12.2. Password construction should include alphanumeric, special characters or punctuation, upper and lower characters.
6.12.3. Avoid the use of dictionary words and proper nouns.
6.12.4. Refrain from using the same password on multiple systems.
6.12.5. DO NOT use passwords utilized on county systems for personal use.
6.12.6. Refrain from storing passwords in a way that does not maintain their confidentiality.

6.13. **USER RESPONSIBILITY IN SECURITY:** Employees are the front line in securing information systems and protecting information. Thus, employees are to take all the necessary precautions to protect Clinton County assets and information. This includes the proper use of county owned technology resources, protection of usernames and passwords, keeping sensitive information clear of desk and screen, proper retention and disposal of sensitive information, and reporting security weaknesses and incidences including violations to county policies. The following items are applicable to all users and employees at Clinton County:

6.13.1. Access to system applications, documentation and data is restricted to authorized individuals.
6.13.2. All access codes, passwords, devices, or other means of gaining access to county owned technology resources and related materials are to be considered strictly confidential. Periodic changing of passwords will be required to maintain confidentiality.
6.13.3. All hardware, software, documentation, and data in both electronic and hard copy form are to be safely and securely stored with access restricted to authorized individuals.
6.13.4. Ensuring sensitive documentation is stored in a secure location.
6.13.5. All electronic files located on the hard drive or on some form of removable media deemed by the user to be critical to the County must also be backed-up to the County's network storage system. Backup frequency should be determined by the critical nature of the data and how often the stored information changes. Data protection (backing up local PC information) is the responsibility of the user. The IT Director will assist as needed.
6.13.6. As with paper documents created and received by an employee, each employee is responsible for retaining electronic records in accordance with the County's retention policy.

6.13.7. Alerting the IT Director when any failure or virus message occurs. If such an event does occur:
- The user should immediately make extensive notes regarding failure.
- Do not turn off the computer.
- If an error message is given, the error message should be copied into the notes.
- If a printer is available and functioning, try to print the screen containing the error message or the screen that will demonstrate the failure.
- The circumstances leading to the failure should be noted, and the notes should be dated and signed.

6.13.8. Alerting the IT Director whenever an unauthorized access attempt or social engineering attempt is encountered. Social engineering attempts include emails from an untrusted source, phone calls in which authentication cannot be granted, unknown media such as CDs, DVDs, or USBs, and any person potentially surveilling the premise.

6.13.9. Protect the data on devices/media entrusted to you by ensuring those devices/media are protected from high temperatures and/or humidity, smoke, dust, food particles and liquid.

6.13.10. Ensure another constituent's information is not in plain view when assisting a constituent.

6.13.11. Close your office door when going to lunch or attending meetings.

6.13.12. Utilize shredding receptacles as appropriate.

6.13.13. Ensure security tokens and outgoing mail are properly secured in an appropriate location.

6.14. **RETENTION:** For the purpose of records retention, e-mail documents are subject to the retention disposal schedule as outlined by the State of Michigan. Disposal of e-mail documents may be suspended should notice of litigation be received by Clinton County. Instructions on disposition of e-mail document retention and preservation will be disseminated by Administration and/or legal representation.

6.15. **DISCLOSURE:** Electronic communications, including but not limited to e-mail documents, are subject to the Michigan Freedom of Information Act to the same extent as and with the same exemptions as those applicable to paper documents. The County reserves the right to inspect any electronic communications found on county owned technology resources for its business activities and to disclose the contents to appropriate personnel.

6.16. **ROLES AND RESPONSIBILITIES:** The IT Director shall be responsible for establishing, maintaining, and monitoring all county provided electronic communication accounts. Requests for new electronic communication access accounts must be approved by the IT Director or his designee.

6.16.1. Each elected official and department head must accept the responsibility to uphold and enforce this policy and subsequent procedures and standards as may be established before electronic communication services are utilized within their respective offices.

6.16.2. It is the responsibility of each user to retain or purge e-mail from their account in accordance with applicable records retention law. Employees will not be held responsible for receipt of unsolicited non-county related e-mail ("spam") but shall be obligated to permanently delete such messages promptly. The IT Department is responsible for the central purging and retention of e-mail on the county file servers. Messages that have been backed up via the normal backup procedure may be retrievable by the IT for no more than 90 days past the deletion. Email backup is designed for disaster recovery, not an archive for each individual message. Limits on storage of items in user's mailboxes will be established by the IT Department. When the established limit is reached in a mailbox, oldest messages will be purged. It is the Individuals responsibility to save any needed e- mail or attachments off the e-mail system. If necessary, the individual shall seek an opinion from their supervisor on the need for retention of business-related e-mail.

6.16.3. Individuals who share their network or internet passwords with others and/or leave their computers unattended and unlocked, may be held responsible for any consequence of unauthorized usage.

6.16.4. Due to the need to protect the County's network from the effects of Malware, all file downloads and e-mail attachments will be virus scanned by county provided anti-virus software at the time of download.

6.17. **VIOLATIONS OF POLICY/COMPLIANCE REVIEW:** Violations of the Electronic Acceptable Use Policy will be evaluated on a case-by-case basis by the IT Director, Administration, and the Elected Official/Department Head. Employees found in violation of this policy will be subject to discipline in accordance with applicable law, labor agreements and departmental rules and regulations, up to and including discharge.

7. **ADMINISTRATIVE PROCEDURES:** The County Administrator is authorized to adjust policy where necessary.

8. **ADMINISTRATOR/LEGAL COUNSEL REVIEW:** The Administrator has determined that this policy as submitted to the Board of Commissioners contain the necessary substance in order to carry out the purpose of the policy. The County Civil Counsel has determined that this policy as submitted contains content that appears to be legal activities of the Clinton County Board of Commissioners.

ELECTRONIC ACCEPTABLE USE POLICY ACKNOWLEDGMENT FORM

This confirms that I have read, understand, and agree to the Electronic Acceptable Use Policy and hereby request access. I understand that County owned technology resources are to be used for conducting the business of Clinton County and that I am not permitted to access a file or retrieve any stored communication other than as authorized in the performance of my job duties. I further understand that all county owned technology resources and all information transmitted by, received from, or stored on County owned technology resources (including e-mail) are the property of Clinton County. I acknowledge that I have no expectation of privacy in connection with the use of this equipment or with the access, transmission, receipt, or storage of information in this equipment, including information for personal purposes.

I acknowledge and consent to Clinton County's monitoring my use of county owned technology resources at any time at its discretion. Such monitoring may include printing and reading e-mail messages entering, leaving, or stored in these systems. I also understand that any violations of the Electronic Acceptable Use Policy may be cause for disciplinary action, discharge from employment, and legal recourse.

Clinton County reserves the right to change or amend its Electronic Acceptable Use Policy at any time, with or without notice.

The following employee/intern/volunteer, by his/her signature, indicates that the Electronic Acceptable Use Policy was read, understood, and agreed to in its entirety. This notice is acknowledged by the employee/intern/volunteer.

Signature: _____

Printed Name:_____ Department:_____

Office Phone: _____ Date: _____

Elected Official/Department Head

I hereby authorize access to the internet and on-line services which are available via the Clinton County account for the Employee/Intern/Volunteer indicated above. My signature below certifies that I have read the Electronic Acceptable Use Policy and that I understand, accept, and will abide by the provisions stated therein.

I accept the responsibility to uphold and enforce this Policy and subsequent Procedures and Standards as may be established, while internet or e-mail services are utilized within my respective office(s).

Signature:_____ Date: _____

REMOTE WORK AGREEMENT

This Agreement is between Clinton County, the Elected Official or Department Head, and the employee ("you"). It must be signed and approved by the employee's Elected Official or Department Head and Controller/ Administrator.

The employee agrees to the following conditions:

A. Clinton County, the Elected Official or Department Head, and you agree that you will temporarily work remote on the following schedule:

Schedule:
(Days of the week, specific hours) _____

Frequency:
(Weekly, every other week, etc.) _____

Accordingly, Clinton County, the Elected Official or Department Head may alter this schedule or end the temporary remote work agreement at any time at its discretion.

B. You agree to maintain a presence with your department while working remotely. Presence may be maintained in the manner and using the technology directed by the department which includes remaining readily available such as by laptop computer, mobile phone, email, messaging application, videoconferencing, instant messaging and/or text messaging always during the times the department expects or requires you to work. You are expected to maintain the same response times as if you were at your regular work location. You will make yourself available to physically attend scheduled work meetings as requested or required by the Department.

C. This remote work arrangement will begin on and will remain in effect unless altered or terminated at any time as described in paragraph A above.

D. While working remote you will work just as if you were in your regular Clinton County Work location and maintain productivity, performance, communication, and responsiveness standards. This Agreement does not change the basic terms and conditions of your employment at Clinton County. You will perform all your duties as set forth in your job description as well as those additional and/or different duties that the Department may assign from time to time. Further, you remain obligated to comply with all Clinton County (as well as the department's) policies and procedures.

E. You will communicate regularly with your office and coworkers which will include a weekly written report of activities as required.

F. If you are a non-exempt (hourly) employee, you are not to work overtime without prior approval

from your Elected Official or Department Head and you are required to take your rest and meal breaks while working remotely in full compliance with federal, state, and local guidelines. You agree to follow such procedures as your manager, or your department head may establish to minimize the likelihood of interruptions or delays to your rest or meal breaks in a way that causes a violation of Clinton County policy. You are required to notify your manager within one business day if you believe you were unable to take a rest or meal break in full compliance with the requirements of federal, state, or local policy on a day on which you worked remotely.

G. You will be solely responsible for the configuration associated with your remote workspace. This includes ensuring and maintaining an ergonomically appropriate and safe remote worksite.

H. All injuries incurred by you during hours you are working and all illnesses that are job-related must be reported. Review the Clinton County's workers compensation policy for more detailed information.

I. You agree that Clinton County equipment will not be used by anyone other than the employee and will exclusively be used for business-related work. The employee will not make any changes to security or administrative settings on Clinton County equipment. The employee understands that all tools and resources provided by the company shall always remain the property of Clinton County.

J. You will use Multi Factor Authentication as setup by County IT.

K. You agree to protect Clinton County equipment from theft or damage and to report theft or damage to your manager immediately.

L. You agree to comply with Clinton County's policies and expectations regarding information security as documented in the Information Security Program and Acceptable Use Policy. The employee will be expected to ensure the protection of all Clinton County information accessible from their remote offices.

M. You understand that all terms and conditions of employment with Clinton County remain unchanged except those specifically addressed in this agreement. This agreement does not change the at-will nature of any at-will employment.

This Agreement is subject to all applicable Clinton County policies, procedures, and collective bargaining agreements. By signing this agreement, you are also confirming you have read, understood. and will comply with all provisions in connection with your remote work arrangement, including but not limited to: Workplace Conduct, Workplace Health & Safety, Conflict of Interest, and the Anti-Harassment and Discrimination Policy.

You acknowledge that if your Elected Official or Department Head deems that the remote work arrangement described in this Agreement is not working effectively or as envisioned, management

may at any time adjust or end the temporary remote work arrangement. Management will strive to provide at least 24 hours advance notice of any changes to the temporary remote work arrangement.

Clinton County will provide appropriate offices supplies (paper, pens. etc.) as deemed necessary and you will be responsible for reporting to your office to pick up those supplies.

Clinton County will provide the following equipment: _____

_____

The employee will provide the following equipment: _____

_____

Acknowledgement

I have read and agree to the terms of the Policy, and I agree to the duties, obligations, responsibilities, and conditions outlined herein.

UNDERSTOOD AND AGREED:

Employee Signature: _____ Date _____

Print Name/Title: _____

ELECTED OFFICIAL / DEPARTMENT HEAD APPROVAL:

Approver Signature: _____ Date: _____

Print Name/Title: _____

Department: _____

CONTROLLER / ADMINISTRATOR APPROVAL:

Approver Signature: _____ Date: _____

Print Name/Title: _____

Department: _____

19950:00001:6443821-1