LEGISLATIVE, RULES & GOVERNMENTAL OPERATIONS COMMITTEE MEETING

LEGISLATIVE AGENDA

January 24, 2023

COMMITTEE MEMBERS:

I. Committee meeting called to order by Chair

II. Approval of minutes of prior Committee Meeting

III. Privilege of the floor and public comment

IV. Action Agenda/New Business Items:

1. Request: To review and approve Warren County Computer Usage Policy and redline changes from November 22, 2022 committee meeting
   Rationale:
   A. The current Warren County Policy on Computer Usage does not fully address management and administration concerns and was updated during the first half of 2022 to reflect clearer policy guidelines for proper use and misuse of the County's computer resources.
   B. The current Warren County Policy does not address accessing data from the computer network and provides clear lines of authority for accessing data at all levels of County government.
   C. Implementing an updated computer usage policy will be the foundation for reviewing and updating the County's FOIL policy.

V. Discussion Items:

1. Request for Proposals: Practice Management Software to Manage FOIL Requests, FOIL Responses, and FOIL Appeals.

VI. Referrals/Pending Items:

VII. Privilege of the floor and public comment

VIII. Motion to adjourn

_____

Attachments: 1.

WARREN COUNTY COMPUTER USAGE POLICY

I. PURPOSE

All computers, servers, cellular phones, storage devices, software, Internet connections, computer applications, voice mail systems, e-mail systems, and any other device used to connect to the County's computer network (collectively referred to as the "computer network") which are supplied by Warren County for use by County employees and agents and are owned and/or licensed by the County of Warren and made available to employees and agents at the sole and unilateral discretion and pleasure of the County of Warren. The County of Warren provides the computer network and access to the computer network for use by employees and agents solely for conducting and engaging in official County business activities only. No County employee or agent possesses any current or future rights in any data, information, programs or files created, modified, and/or stored on the computer network and all such data, information, programs, and files are and remain the sole legal property of the County of Warren.

As established by Board of Supervisors Resolution 409 of 2014, the County's computer network system and voice mail systems are intended for the business use of Warren County personnel and agents. Any use of the computer network by any other persons, unless specifically and expressly permitted by Warren County is unauthorized. All records (including email and voice mail and other messages) generated or stored on the computer network are County-owned records. The County reserves the right to access and disclose, at any time and for any purpose, all records sent over or stored in its computer and/or systems. The use of the County computer network constitutes that person's consent to the County's right to access and disclose data from the computer network.

While our direct connection to the internet offers a cornucopia of potential benefits in performing our day-to-day work activities, it also opens the door to significant risks to our data and systems if we do not follow appropriate security measures and discipline while interacting with our computer systems. As presented in greater detail below, security may require that computers with sensitive data or applications, shall not connect to the internet, have restricted access to the internet, or that certain officers and employees must be prevented from using certain Internet features like file transfers. The overriding principle is that computer security is everyone's first concern. An officer or employee may be held accountable for any breaches of the security measures set forth by this policy, or for violating confidentiality requirements through the unauthorized release of County-owned computer information and data.

Certain terms used this policy should be understood in their customary usage and be read to include the broadest possible meaning and to include their related concepts:

- "Computer network" means All computers, servers, cellular phones, storage devices, software, Internet connections, computer applications, voice mail systems, e-mail systems, and any other device used to connect to the County's computer network
- "Document" covers just about any kind of file that can be read on a computer screen as if it were a printed page and includes any electronically stored data, including HTML files read on an Internet browser, any file meant to be accessed by a word processing or desk-

top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

- "Data" means any information, knowledge, facts, concepts or instructions which is processed on a computer network and includes data in any form, whether readable by a computer or a human and wherever stored on the County's computer network.
- "Graphics" includes photographs, pictures, animations, movies, or drawings.
- "Display" includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

The County will provide Internet access to those employees who demonstrate a legitimate business need. County employees and agents granted computer access, email access and/or Internet access as part of their employment shall be provided with a copy of this policy and shall acknowledge receipt of this policy and the requirement to know the contents of the policy while employed by the County.

II. INTERNET POLICY PROVISIONS

A) Management and Administration

1. The County has software and systems in place that monitor and record all Internet usage. We want you to be aware that our security systems have the potential to record (for each and every user) each World Wide Web site visit, social media usage, email messages, and each file transfer into and out of our internal networks. The County reserves the right to record all such activity which occurs upon the County computer systems and the right to review such activity and data at any time, as provided for by this policy. No employee possesses, or should possess any expectation of privacy as to his or her computer network activity and usage while using the County's computer network. Periodic review of computer network activity will analyze usage patterns by employees to ensure that the County computer network is used by employees to maintaining the highest levels of productivity, and security.
2. The County reserves the right to inspect any and all files downloaded from any source, to include the Internet, which are stored on the County's computer network in order to assure compliance with this policy.
3. Since a wide variety of materials may be deemed offensive by co-workers, vendors, suppliers or members of the general public, it is a violation of County policy to store, view, print or redistribute any document or graphic file that is not directly related to the user's job or the County's business activities
4. The receipt, storage, or display of any visual depiction of nudity[1] on the County's computer network is strictly prohibited, unless required for the performance of the employee's official duty (i.e. law enforcement officers assigned to the Sheriff's Office). In addition, no visual depiction of nudity, to include pornography or sexually explicit conduct shall be archived, stored,

[1] As the term is defined by Penal Law section 235.20(2) to mean the showing of the human male or female genitals, pubic area or buttocks with less than a full opaque covering, or the showing of the female breast with less than a fully opaque covering of any portion thereof below the top of the nipple, or the depiction of covered male genitals in a discernably turgid state.

distributed, edited or recorded using the County's computer network, unless required for the performance of the employee's official duty.

5. The County actively uses software to identify Internet sites which host or maintain inappropriate and/or sexually explicit visual depictions. The County may block access from within our computer network to all such sites identified by the County. The failure of the County to identify and block access to an Internet site which contains inappropriate and/or sexually explicit material does not permit or condone an employee from accessing such sites while using the County's computer network. If an employee accidentally connects to a website that contains inappropriate and/or sexually explicit material, you must disconnect immediately from that website.

6. This County's computer network shall not be used to violate the laws and regulations of the United States, or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction. Use of the County's computer network for any illegal activity is grounds for disciplinary action, to include possible termination. The County shall cooperate with and comply with all reasonable requests from law enforcement agencies relating to an investigation and/or lawfully-issued subpoena.

7. Employees using the County's computer network shall be aware of laws involving copyright protections, trademarks, libel, and public speech control laws of all agencies in which this County maintains a business presence to avoid County liability from an inadvertent violation of such laws.

8. Employees may download software for direct business use, only after Department Head approval and approval by the Director of Information Technology. The employee and Department Head shall arrange to have such software properly licensed and registered to the County. Any software or files downloaded from the Internet to the County's computer network becomes the property of the County. Any such files or software shall be used only in ways that are consistent with their licenses or copyrights, and for official County business.

9. The County's computer network shall be used for county business only. Prohibited downloads and nefarious uses include but are not limited to: knowingly downloading or distributing pirated software or data; deliberately propagating any virus, worm, Trojan Horse, trap-door program code; crypto-mining; circumventing systems intended to protect the privacy or security of any computer network user; and using the County's computer network to disable or overload any computer system or network, to include the County's.

10. No employee or agent shall use the County's computer network to conduct any form of gambling.

11. Employees and agents shall not use the County's computer network to download entertainment software or games.

12. County employees and agents shall identify themselves honestly, accurately and completely (including one's County affiliation and function when requested) when using the County's computer network, to include, setting up accounts on outside computer systems, unless~~,~~ required for the performance of the employee's official duty (i.e. law enforcement officers assigned to the Sheriff's Office).

13. The County owns all data and material created and posted by a County employee and agent to any forum, social media or World Wide Web page in the course of their official duties. The County shall own and possess all legal rights to copyright, trademark, license and control the use and distribution of such data and material.

14. Employees and agents shall not upload any software owned by the County or

licensed to the County, without the prior written approval of the employee's Department Head, the written approval of the Department Head responsible for such software, and the Director of Information Technology.

15. Any on-line presence (i.e. social media page for business purposes) must first be approved by the Department Head, Director of Information Technology, County Administrator and the Oversight Committee for the employee's department. Content posted shall require access and oversight by the Department Head and the Director of Information Technology, or other persons designated by the Director.

16. Employees and agents are reminded that social media is a public forum where it is inappropriate to reveal confidential County information. Employees and agents releasing protected information via social media - whether or not the release was inadvertent - may be subject to disciplinary action, to include termination of employment, as stated by County policies and procedures.

17. Use of the County's computer network to violate County policies or commit criminal acts or non-criminal violations, such as misuse of County resources, sexual harassment, and misappropriation or theft of County property are strictly prohibited by this policy and other related County policies.

18. E-mail is a strategic business tool to facilitate communication between County employees, other State and local municipal employees, County vendors, customers, business, and members of the general public. Warren County's e-mail systems are the exclusive property of the County and are owned by the County or licensed from third-party vendors. E-mail systems and the data created are the sole and exclusive property of the County. and are intended to be used for official County business. All messages sent or received via e-mail are County property. It is against County policy to use e-mail for any unlawful endeavor.

B) <u>Technical</u>

1. User ID's and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. County policy prohibits the sharing of user ID's or passwords obtained for access to Internet sites.

2. Employees and agents should schedule communications-intensive operations such as large file transfers, video downloads, and the like for off-peak times and only after approval from Director of Information Technology.

3. Mass emailing (other than email groups created for business purposes) should not be done from a county email address. If there is a business-related need for mass emails, the Information Technology department should be consulted as to identify an appropriate third-party service.

C) <u>Security</u>

1. The County has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the County's networks. Any employee or agent who attempts to disable, defeat or circumvent any County security facility (for example, by utilizing a personal VPN) will be subject to immediate disciplinary action.

2. No employee or agent shall transfer any sensitive computer network data outside

the County's computer network without Department Head approval, and only for official business purposes within the scope of the employee's duties and responsibilities. No elected officer, appointed officer, or Department Head shall transfer any sensitive computer network data outside the County's computer network unless for official business purposes. All transfers of sensitive County computer network data outside the County's computer network shall be encrypted prior to distribution, whether sent by way of the Internet or upon other physical storage devices. 3.

Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connection to any outside computer can be used by an attacker to compromise any County network to which that computer is attached. That is why any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the County's internal networks.

4. Only those Internet services and functions with documented business purposes for this County will be enabled at the Internet firewall.

5. No employee is permitted to connect to the County's computer network from an outside source, such as Webmail or Virtual Private Networks (VPN), unless:

- The connection is authorized by the Department Head and the IT Department; and
- The connection is established using the two-factor authentication ("2FA") ~~required for the County's computer network~~; and
- Only County-approved devices shall be used to connect to the VPN~~Any VPN connection using 2FA must be made using an approved County device~~ (no personally owned devices); and
- Any exceptions to these requirements may be made under exceptional circumstances, and on a case-by-case basis with the pre-approval of the Department Head and IT Department (i.e. County-wide emergency requiring increased access through non-County approved devices.

III. PASSWORD REQUIREMENTS

1. All passwords used by County officers and employees to access~~ing~~ County network, data or information systems must be kept secure. As such the following specific criteria must be met for every password:

a. Passwords are not to be written down or stored in an unencrypted form;
b. Temporary passwords must be changed upon first use;
c. Passwords must be a minimum of 8 characters in length; and
d. Passwords must also meet the following requirements;
   i. They do not contain all or part of the user's account name or common word; and
   ii. Passwords must contain characters from each of the following 3 categories:
      1) English uppercase characters (A through Z);
      2) English lowercase characters (a through z); and
      3) Base 10 digits (0 through 9).

2. County officers and employees shall only access the County's computer network

by use of their individually-assigned password.

3. No County officer or employee shall share their password to access the computer network with any non-employee or member of the general public.

4. No County officer or employee shall share their password to access the computer network with any County officer or employee, to include their supervisor, department head, or any member of the IT Department.

~~3.~~5. Under no circumstances shall any County officer or employee request from another officer or employee their password to access the computer network. Specifically, no supervisor, department head, or member of the IT Department shall request from any County officer or employee their password for access the computer network.

Formatted: Indent: Left: 0", First line: 0.5"

IV. ACCESS TO COMPUTER NETWORK DATA

A) County employees may access data from the computer network which is necessary for the employee to perform the official business of the County within their assigned duties and responsibilities, as determined by the employee's Department Head or County Administrator. Accessing County data from the computer network for any non-official business purpose or data outside an employee's assigned duties and responsibilities is strictly prohibited and may result in disciplinary action.

B) The Director of the Information Technology Department, or the designee from within the IT Department, shall be the only County officer or employee authorized to access email archives when authorized by this policy.

C) All requests to access email archives shall be in written form to the Director of IT, or his designee.

~~B)~~D) For official business purposes only, County Department Heads may access data from the computer network for any employee under their Department's supervision, or may request and receive data from the email archives for employees in the Department.

~~C)~~E) For official business purposes only, the County Administrator, Director of Human Resources or County Attorney may direct the Director of Information Technology to search, retrieve and provide data from the computer network based upon any County employee's name or other unique method of identification (i.e. email address, employee identification number, etc.), except for County elected officers, upon providing, in written form~~ing~~, the specific business purpose for which the data is required.

~~D)~~F) The County Administrator, Director of Human Resources, or County Attorney may request~~access~~ data from the computer network using the name or other unique method of identification for a specific elected County officer~~for any elected County officer only~~ by use of the following procedure:

1. Provide a written request to the Director of Information Technology for computer network data ~~based upon the name or other unique method of identification for a specific elected County officer~~ stating the specific business purpose for which the data is required (i.e. ~~FOIL response,~~ lawsuit discovery disclosures, administrative complaint and investigation, investigation by Board of Ethics, etc.);
2. Contemporaneously provide a copy of the written request to the elected offic~~er~~ial~~;~~;
3. Obtain the written consent of the County Administrator, Director of Human Resources and~~/or~~ County Attorney, prior to releasing the computer network data requested.

4. This limitation on accessing computer network data for a specific County elected ~~official~~ officer shall not apply to IT-assisted searches for data using keywords which are not an elected offic~~erial~~'s name or other individual method of identification (i.e. email address, employee identification number, etc.).

~~4.~~5. This limitation on accessing computer network data for a County elected officer shall not apply to the requests by a Record Access Officer complying with the requirements of Public Officer Law, Article 6, Freedom of Information Law.

~~E)~~G) For official business purposes only, the ***[which one may request???]*** **Chairperson and/or Committee Chair and/or Supervisor** _____ of the Board of Supervisors may direct the Director of Information Technology to access data from the computer network generated by~~fo~~r the County Administrator, Clerk of the Board of Supervisors, County Attorney, County Auditor, County Public Defender, and County Purchasing Agent, or for any employee of those Departments, only by use of the following procedure:

1. Provide a written request to the Director of Information Technology for computer network data based upon the name or other unique method of identification for a specified appointed County officer~~.~~, or member of their department, stating the specific business purpose for which the data is required;
2. Obtain the written consent of the ~~Chairperson of the Personnel Committee,~~ County Administrator, Director Human Resources~~,~~ and County Attorney. No consent shall be required from an appointed County officer if they are the employee whose data is being requested.
3. If the computer network data of the County Attorney, District Attorney, Public Defender, or its employees is being requested by the _____ ~~Chairperson~~, then the Director of Information Technology~~ies~~ shall release the data directly to the County's outside retained counsel for labor relations for a confidential review of the data to ensure no release of attorney-client communications or other privileged work product and confidential information, prior to ~~is~~ release~~d~~ to the _____ ~~Chairperson~~, and all attorney-client communications or other privileged work product and confidential information shall be removed or redacted, prior to release to _____ ~~the Chairperson for the Board of Supervisors~~.

~~3.~~4. If the computer network data of the Director of Human Resources, or its employees is being requested by the _____, then the Director of Information Technology shall first release the data to the County Attorney for a confidential review of the data to ensure no release of Health Insurance Portability and Accountability Act (hereafter, "HIPAA") protected data, data protected under New York's Personal Privacy Protection Law, or confidential information and data related to any investigations and/or actions taken under section 75 of the Civil Service Laws, Warren County Workplace Violence Prevention Plan and Program, or the Policy Against Discrimination and Harassment for Warren County.

~~F)~~H) Unauthorized access to the County's computer network and data by an employee or agent is strictly prohibited and may result in disciplinary action, to include discipline up to and including termination of employment for an employee, and public censure if an elected official.

~~G)~~I) Nothing in this policy restricts or limits access to the County's computer network data and obligation to comply with a lawfully issued Court-ordered search warrant, ~~or~~

Formatted: Font: Bold, Italic

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

lawfully issued and served subpoena *duces tecum*, or ;the request of a Records Access Officer of FOIL Appeals Officer when responding to a FOIL request or FOIL appeal.

V. VIOLATIONS OF COMPUTER USAGE POLICY

1. Every County officer and employee shall receive a copy of the computer usage policy and complete the attached acknowledgement within thirty (30) days of the effective date for the policy.

2. Prior to any newly elected, appointed or hired County officer or employee receiving access to the County computer network they shall sign the acknowledgement attached to this policy and provide it to Human Resources in care of the IT Department.

3. Violations of the Computer Usage Policy may result in the filing of a criminal complaint against an employee, and disciplinary action against the offending non-elected County officer or employee, which may include: reprimand, fine not exceeding $100 to be deducted from the salary of the employee; suspension without pay for a period not exceeding two months; demotion in grade and title; or dismissal from employment.

4. Violations of the Computer Usage Policy may result in the filing of a criminal complaint against the elected officer, and disciplinary action, which may include any lawful action provided under Public Officers Law, or by rule or resolution of the Board of Supervisors.

[REMAINDER OF PAGE INTENTIONALLY OMITTED]

Formatted: Font: Bold

Formatted: List Paragraph, Centered, Numbered + Level: 1 + Numbering Style: I, II, III, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.75"

Formatted: List Paragraph

~~Please read and sign the following statement and return the original signature page to IT.~~

ACKNOWLEDGEMENT OF WARREN COUNTY COMPUTER USAGE POLICY

Formatted: Font: Bold

Formatted: Centered

"I have received and reviewed a complete written copy of Warren County's Computer Usage Policy, effective ~~August~~ _____, __, 202~~2~~3, per Board of Supervisors Resolution ___ of 202~~2~~3 (hereafter, "Computer Policy"). I fully understand and acknowledge the terms of this Computer Policy and shall abide by each any every requirement stated by the Computer Policy.

I acknowledge and accept that the County's security software will record data I create, modify, store and transmit on the County's computer network, as well as the Internet address/IP address of any Internet site that I visit and will keep a record of all network activity in which I transmit or receive any kind of data.

I acknowledge and accept that any message or data I send or receive, to include but not limited to emails and text messages on the County's computer network, will be recorded and stored in an archival system and may be access by authorized County officers, employee~~'~~s or agents for use by County management.

I acknowledge and accept that violations of the Computer Policy may result in disciplinary action or even criminal prosecution under State or Federal criminal laws.

I acknowledge and agree that any use of County owned, leased or licensed computer equipment and/or software for Internet access constitutes consent to the County's monitoring, recording and inspection of all data, to include but not limited to downloaded files, e-mails, and text messages, as set forth in this policy.

Failure to sign and return this policy to IT will result in immediate denial of all access to the County computer network."

_____

Signed **Date**

_____

Print Name **Department**