Warren County Board of Supervisors

RESOLUTION NO. 80 OF 2026

RESOLUTION INTRODUCED BY SUPERVISORS RUNYON, CROCITTO, DRISCOLL, ETU, MADAY, TURNER AND CONOVER

ADOPTING THE WARREN COUNTY COMPUTER USE POLICY

WHEREAS, the Risk and Safety Committee recommended and the Personnel & Higher Education Committee agreed to adopt the Warren County Computer Use Policy and recommended that the same be advanced to the Board of Supervisors for consideration and approval, now, therefore, be it

RESOLVED, that the Warren County Computer Use Policy, annexed hereto as Schedule "A," be and the same is hereby adopted as the official policy for Warren County, and be it further

RESOLVED, that any and all prior Warren County Computer Use Policies, Resolutions or parts thereof inconsistent with the annexed Warren County Computer Use Policy are hereby repealed effective February 20, 2026.

EXHIBIT A: COUNTY OF WARREN, NY COMPUTER USE POLICY TERMS

I. PURPOSE

The County of Warren, herein after referred to as County, supports information assets that process electronic data. The purpose of this policy is to define the requirements and responsibilities that all users must follow. This policy is drafted to provide awareness and notification of what the County deems to be acceptable and unacceptable use to avoid compromise of County systems, services and legal issues.

II. DEFINITIONS

Authorized County Computer Use: Computer use authorized by the County for work duties for County operations and business.

Biometric Data: Personal information stored by the County regarding an individual's physical characteristics that can be used to identify a person, such as fingerprints, voiceprints, facial shape, or scan of hand or face geometry as defined by applicable state and federal laws.

Biometric Identifier Information: A physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic.

Browser Cookies: Small text files that websites store on a computer to remember information about you, such as login details, shopping cart items, and preferences to personalize your web browsing experience.

Collaborative Software: A type of application that enables multiple people to work together on projects, share information, and communicate seamlessly, regardless of their physical location. Also known as groupware, it supports tasks like communication, coordination, and problem-solving through features such as instant messaging, document sharing, and video conferencing.

Computer Hardware Setup: The installation of computer hardware including computers, printers and scanner and their configuration to the Town's computer network.

Computer Data Network: A network system of two or more interconnected computing devices that communicate and share data, resources, and services.

Computer Software: A set of instructions, data or programs that tells a computer's hardware what to do and how to perform.

Computer User: An individual or entity that interacts with a computer system, network, or software to perform tasks, access information, or utilize services.

Confidential or sensitive business data: County documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual, outcome of a charge/complaint/case, the County or third parties' proprietary information, or the County's financial operations.

County Code of Ethics Legislation: The Warren County Ethics and Disclosure Law, as approved and enacted by the County Board of Supervisors.

County IT Basic Support Hours: The regular business hours of the County IT staff Monday through Friday from 8:00AM to 5:00PM.

Cyber Threat: Any event, action, or circumstance with the potential to negatively impact an organization or individual's digital assets, systems, or data through unauthorized access, damage, or disruption.

Cyber Security Training: Online specialized computer awareness training to educate end users about protecting computer systems, networks and data from attacks by outside parties.

Department Head: Each elected and appointed County officer responsible for the administration of their respective departments, agencies and offices which collectively constitute the structure of the County's governmental operations.

Department Head Designee: A County employee with statutory authority or designated by the Department Head to act on their behalf.

Data: Information, knowledge, facts, concepts or instructions which are generated, processed or stored on a desk top VOP phone, computer network, in any form, whether readable by a computer or a human wherever located.

Employee: A person employed by the County of Warren on a full-time, part-time, less than part-time, per diem, or seasonal/temporary basis, and includes volunteers and interns, whether paid or unpaid.

Employer: The County of Warren ("County").

Endpoint Device: Any device that connects to and communicates with a network, such as a desktop computer, laptop, smartphone, tablet, server, or Internet of Things (IoT) device.

Endpoint Protection: Computer security measures that defend devices, known as endpoints, such as laptops, smartphones, and servers, from cyber threats and malicious attacks.

Firewall: A part of a computer system or network which is designed to block unauthorized access while permitting outward communication.

Identity Theft: Fraud committed or attempted using the identifying information of another person without their permission.

Internet of Things (IoT) Device: A physical object, such as a sensor, appliance, or gadget, that connects to a network, like the internet, to transmit and exchange data without human intervention.

Mass Emailing: An email and/or email campaign pertaining to County business sent to a large group of recipients of over one hundred (100) or more outside of the County's computer network.

Minimum Applications and Services (IT MAAS): Minimum IT applications and services established by the County IT in concert with the County's Insurance requirements that include core functions like account management, patching, data backup, secure storage, network access, and fundamental security tools like firewalls.

Minimum System Requirements: The essential hardware and software specifications—such as processor, RAM, storage, and operating system identified by the County IT Department that is needed for a piece of software or hardware to function at a basic level, though often with slower performance than recommended levels.

Mobile Device: A small, portable, handheld computing device powered by a battery, designed for wireless communication and general computing on the go, featuring a display (touchscreen) and internal storage.

Multifactor Authentication (MFA): A security system that requires more than one type of proof to verify a user's identity, making it significantly harder for unauthorized access than a password alone.

Network Management: The comprehensive process of configuring, monitoring, and maintaining a computer network's infrastructure to ensure its efficient, reliable, and secure operation. It involves using tools and processes to manage network devices like routers and switches, provision resources for users and applications, monitoring performance, and responding to faults and security threats.

Network Operating System (NOS): Specialized software that allows multiple computers to communicate and share resources on a network, such as files, printers, and internet access. It manages network resources, provides network security, and supports both client-server architectures (where dedicated servers provide resources) and peer-to-peer networks (where devices share resources directly).

Network Structure: The physical and logical design that determines how devices connect, communicate, and share resources using hardware, software, and protocols.

Officer: An individual given the title of Officer for the County of Warren.

Personal Device Use: Computer, smart phone, tablet, or other device that is authorized to access County Data or is used to backup any such device and is owned by a private individual and acquired voluntarily, without payment by the County and without any expectation of reimbursement for any costs related to the purchase, activation, operational and connectivity charges, service or repairs, or other costs that may be incurred related to the device or its use.

Personal Electronic Device: Personal privately owned portable electronic devices used by individuals for communication, information, and entertainment, including smartphones, tablets, laptops, and smartwatches.

Personal Identifiable Information: Information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means, to include information that directly identifies a person, such as a name, address, social security number, telephone number, email addresses, or by which the County may identify a specific person in conjunction with other data such as gender, race, birth date, or other descriptors.

Phishing: A cybercrime in which a target or targets are contacted by email by someone posing as a legitimate institution or person to lure individuals into providing confidential information, such as County Sensitive Information, that will be used for unlawful and malicious purposes.

Principle of Least Privilege (POLP): A cybersecurity concept that requires users, systems, and applications to have only the minimum level of access and permissions necessary to perform their specific, authorized tasks.

Red Flag: A pattern, practice or specific activity that indicates the possible occurrence of identity theft.

Remote Access: The ability to connect to and control a computer, network, or system from a different geographical location, allowing users to perform tasks such as accessing files, running applications, and managing systems without being physically present.

Sensitive Information: Any personal identifiable information collected by the County for a stated purpose in which the risk of identity theft is present.

Server Management: The ongoing process of maintaining, monitoring, and optimizing server hardware and software to ensure high availability, performance, security, and scalability. Key activities include server monitoring, software

updates, security configuration, backup and recovery, and hardware maintenance to keep servers running efficiently and to protect data.

Shared Services Partner(s): A municipality within the County of Warren that has contracted for Information Technology Services and agreed to abide by the terms and conditions of this County policy.

Social Networking Sites: Online platforms where computer users create profiles to connect with other people, build social networks, and share information.

Third Party Service: Any unaffiliated person, company or entity that performs services for a company that is paid for their services, but does not have a stake, share or equity in the company.

Unauthorized Computer Access: The act of accessing computer systems, networks, or data without explicit permission or authorization from the system owner. This violation of security policies can involve methods like gaining entry through security loopholes, guessing passwords, or using malicious code to gain access to systems, data, or other resources without consent.

Unauthorized County Computer Use: Illegally accessing a computer or computer network or allowing another person to have access without the permission granted by the County.

Vendor: An individual or company that contracts with the County for the provision of goods and/or services in accordance with the County's Purchasing Policy.

Vendor Computer System Support: The technical assistance, maintenance, and services provided by the external manufacturer or software provider (the vendor) of a specific computer hardware or software product, often to resolve complex, product-specific issues that an organization's internal IT team cannot handle on its own.

Workplace: Any location where an employee performs any work-related duty in the course of their employment.

Workstation Troubleshooting: The systematic process of identifying the cause of a problem within a computer workstation, diagnosing the fault, and implementing a solution to restore it to its normal working order.

EXHIBIT B: COUNTY POLICY GOVERNANCE

I. Purpose:

The County provides data access for use by employees and the County's agents for the sole purpose of conducting and engaging in official County business. No County employee, officer or agent shall possess any current or future rights to any data created, modified, and/or stored on County systems and all such data shall remain the sole legal property of the County. The use of County systems constitutes an individual's consent to the County's right to access and disclose data as deemed legal and appropriate by federal, state and local law. The County shall provide data access to those employees, officers and agents who meet the criteria of the County's computer use policies and agree to its terms and conditions.

II. County Computer Use Management and Administration:

The County has systems in place that monitor and record all data use. The County reserves the right to record all such data activity which may occur within the County's systems and reserves the right to review such activity and data at any time as may be needed for the County's legal purposes, as provided by this policy. It also reserves the right to inspect any and all files downloaded from any data source which may be stored on County systems which may be found to be in violation of state or federal law. County Department Heads and/or their designees shall be responsible for assisting the Department of Information Technology with enforcing the terms and conditions of their employee's use of County data systems.

The County Director of Information Technology shall be designated as the Administrator of the County's data systems and their implementation under the reporting supervision of the County Administrator. The County Director of Information Technology, as a member of the County Risk and Safety Committee shall make regular reports to the Committee regarding the status of the County's cyber security controls, security issues, and cyber incidents as they may occur.

The following rules shall govern an individual's use of the County's computer network:

1. **County Departments Governed by Federal and/or State Requirements:** County departments, including but not limited to the Department of Social Services, and Warren County Sheriff's Office, utilizing federal and/or state email and data systems shall be required to meet the standards set by those government requirements which shall supersede the County's Computer Use Policy in the event of a conflict of terms and/or conditions.
2. **Username:** Employees, officers and agents of the County shall be provided with a unique username and temporary password used to gain initial access to County systems as may be needed to perform their job responsibilities. Each user shall then be required to individualize their password. The sharing of user ID's or passwords is prohibited
3. **County Emails:** Employees, officers and agents of the County shall be provided with a unique County email address consistent within the WarrenCountyNY.gov nomenclature to conduct County business as requested by the Department Head or County officer consistent with their job responsibilities.
4. **Passwords:** All passwords used by County employees, officers and agents for access to County systems must be kept secure. No user should share their password. This shall include their supervisor, department head or any member of the Information Technology Department.
5. **Mass Emails:** Mass emailing (other than email groups created for business purposes) shall not be sent from a County email address. If there is a business-related need for mass emails, the Department of Information Technology should be consulted to identify an appropriate third-party service
6. **Blocked Internet Sites:** The County attempts to actively identify and block Internet sites which host inappropriate cultural, discriminatory, and/or sexual depictions in accordance with statutory regulations pertaining to workplace harassment and workplace violence. The failure of the County to identify and block

such sites does not permit or condone users from accessing such sites. If a user accidentally connects to such a website, the user is expected to immediately disconnect from that website.

7. **Lawful Use:** County systems 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 County systems for any illegal activity is grounds for disciplinary action including termination. The County shall cooperate with and comply with all reasonable request from law enforcement agencies relating to an investigation and/or lawfully issued subpoena of any data records contained within its systems.
8. **Software:** Users may install software for official County business use, only after the approval of the employee's Department Head and the Director of Information Technology. The Department Head with the assistance of the Department of Information Technology shall arrange to have such software properly licensed and registered to the County. Any such software shall be used only in ways that are consistent with their licenses and/or copyrights.
9. **County Data Systems:** The Director of Information Technology shall be named as the County's Administrator for all critical data systems including financial, operational, and security data systems. Application for access should be made to the Department Head governing the software and be directly related to job responsibilities. If approved, the Department Head shall forward the application for data system access to the Director of Information for Technology for installation. If the access request is denied by the Department Head controlling the data system in question, the Department Head requesting access shall forward the written request and the denial to the County Administrator for a final determination as to whether or not access to said data system should be granted. In this case, the Director of Information Technology shall abide by the decision made by the County Administrator.
10. **Security:** The County has installed a variety of security systems to ensure the safety and security of the County's systems. Any employee, officer or agent who attempts to disable, defeat or circumvent any security system (for example, by utilizing a personal VPN) shall be subject to immediate disciplinary action. No employee, officer or agent shall transfer any sensitive data containing personal identifying information governed by federal and state law outside the County's systems 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 data containing personal identifying information governed by federal and state law outside the County's systems unless for official business purposes.

III. Access to County Computer Network Data:

1. No request by a County officer or employee for access to the County's computer network data, to include emails, shall be authorized unless made in written form and authorized to be released by any one of the following three criteria:

    a. **Department Head Requests:** Department Heads are authorized to request access to computer network data for an employee assigned to that Department Head's department. A Department Head seeking computer network data for employees within their department shall submit a written request to the Director of Human Resources for review and approval, who may, as needed, consult with the County Attorney's Office. The written request for the County's computer network data shall state the name of the employee, the date or date range for data requested and a statement of the business reason for the request. The Director of Human Resources shall provide the Director of Information Technology with any approved requests to release the computer network data to the requesting department head.

    b. **County Administrator/County Attorney/Director of Human Resources Requests:** The County Administrator, County Attorney and Director of Human Resources each may require the Director of Information Technology to search, retrieve and provide computer network data, for any County officer, employee, or agent, by name or other unique method of identification (i.e. email address, employee identification number, etc.), and each such request shall be in writing and state the business purpose

for which the data is required..

c. **Freedom of Information Law Requests:** A written request for computer network data submitted by the Records Access Officer, a Designated Department Head under FOIL, or the FOIL Appeals Officer when responding to a FOIL request or appeal shall be valid when made to the Director of Information Technology through the NextRequest FOIL management system in response to an active FOIL request or appeal and the data is needed to comply with New York State FOIL requirements and the County's FOIL policy.

2. The Director of Information Technologies shall maintain a log of all requests for computer network data access, except for requests made pursuant to FOIL, for eighteen (18) months after the request is submitted, which preserves the name of the requestor, the date of the request, the data requested, and the data provided. Access to the log of all requests shall be provided, upon request, to the County Administrator, County Attorney or Director of Human Resources.

3. Nothing in this policy restricts or limits access to the County's computer network data and the County's obligation to comply with a lawfully issued Court-ordered search warrant or other Court order, lawfully issued and served subpoena or other lawful process

IV. **Reporting of Cyber Liability Issues:** Any user given access to the County's data system shall be responsible for the reporting of a cyber threat to the County's Information Technology Department upon learning of the threat. The County Director of Information Technology and/or Department Heads shall be responsible for IMMEDIATELY reporting cyber liability incidents that materially impact County operations, confidential and privileged information including personal identifying information, and financial integrity incidents to the County Administrator and County Attorney.

V. **County Policy Use Acknowledgement:**

1. Prior to any newly elected, appointed or hired County officer or employee receiving access to the County computer network they shall be required to sign the **"County Computer Use Policy Acknowledgement" (Attachment A)** and provide it to the Department of Human Resources.
2. Within thirty (30) days of the adoption of a revision to the County Computer Use Policy, every county employee, officer and agent shall receive a copy of the revised policy and shall acknowledge receipt of the policy either through the WC Application Portal or by signing the "County Computer Use Policy Acknowledgement" (Attachment A) and providing same to the Department of Human Resources.

VI. **County Discipline of Violations of County Computer Usage:**

Unauthorized access to the County's computer network and data by an employee, officer or agent is strictly prohibited and may result in disciplinary action, including discipline up to and including termination of employment for an employee, and public censure if an elected officer. Violations of the Computer Usage Policy may result in the filing of a criminal complaint against:

1. an employee, and disciplinary action against the offending non-elected County officer or employee, which may include reprimand, fine not exceeding One Hundred Dollars ($100) to be deducted from the salary of the employee; suspension without pay for a period not exceeding two (2) months; demotion in grade and title; or dismissal from employment; OR
2. 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.

EXHIBIT C: CYBER INDUSTRY GENERAL STANDARDS FOR THE COUNTY AND ITS SHARED IT SERVICES PARTNERS

The County Director of Information Technology shall be designated as the Administrator of the County's data systems and their implementation to include Shared Services IT Partnerships under contract with the County. The County Director of Information Technology, as a member of the County Risk and Safety Committee shall make regular reports to the Committee, and Board of Supervisors and Shared IT Services Partners governing bodies regarding the status of the County's cyber security controls, security issues, and cyber incidents as they may occur.

County departments and/or Shared Services IT contracted partners, including but not limited to the Department of Social Services, local law enforcement, emergency services organizations, and the Warren County Sheriff's Office, utilizing federal and/or state email and data systems shall be required to meet the standards set forth by those government requirements which shall supersede the County's Computer Use Policy in the event of a conflict of terms and/or conditions.

The following cyber industry criteria shall set the minimum technology requirements for cyber security protocols for use of the County data systems:

I. **Public Use of the County System:**

Any member of the general public who connects to the County and Shared IT Services Partners' Public Wireless Network in order to use it directly or to connect to any other network(s), must shall be required to comply with the following provisions as posted to the County website and agree to comply with this Policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules and regulations. The following notification with a request of acceptance shall be required of all public wireless users:

THE COUNTY AND ITS SHARED IT SERVICES PARTNERS MAKE NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE PUBLIC WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS.

The County and its Shared IT Services Partners take no responsibility and assume no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Public Wireless Network. The County and its Shared IT Services Partners reserve the right to disconnect any user at any time and for any reason. The Public Wireless Network is provided as a courtesy to allow our visitors access to the internet.

Inappropriate use of the Public Wireless Network is not permitted. The County and its Shared IT Services Partners present the following inappropriate uses as examples of guidelines as listed below:

- ***Users must respect the privacy and intellectual property rights of others.***
- ***Users must respect the integrity of our network and any other public or private computing and network systems.***
- ***Use of the Public Wireless Network for malicious, fraudulent, or misrepresentative purposes is prohibited.***
- ***The Public Wireless Network may not be used in a manner that precludes or hampers access by other users to the Public Wireless network or any other networks.***
- ***Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host or network.***

II. Privacy and Monitoring:

By using the Internet access provided by County and its Shared IT Services Partners, users who utilize County and/or Shared IT Services Partners owned and/or maintained computer devices shall be required to agree to this policy and acknowledge that records of Internet access, such as sites visited, images reviewed, and email sent, may be recorded and monitored by the County's Information Technology Department at any time with no expectation of privacy and that:

1. Encrypted technology that meets our requirements will be employed.
2. The County and its Shared IT Services Partners own the rights to all data and files in its computers, network, or other information systems, subject to applicable laws. Users may not access networks, servers, drives, folders, or files to which the user has not been granted authorization. Users may not destroy, delete, erase, or conceal files or other data, or otherwise make files or data unavailable or inaccessible. In addition, users may not access another employee's computer, computer files, or electronic mail without authorization from their supervisor.
3. The County and its Shared IT Services Partners use of certain licensed commercial software application programs from third parties for business purposes. Third parties retain the ownership and distribution rights to this software. Users may not use or distribute licensed software.
4. Electronic mail ("email") messages sent and received using our equipment or Internet access provided by us are not private and are subject to viewing, downloading, inspection, release, and archiving by us. The County and its Shared IT Services Partners reserve the right to inspect files stored in private areas of the County and its Shared IT Services Partners' network or on individual computers or storage media to assure compliance with our policies and applicable state and federal laws. It may monitor electronic mail messages (including personal/private/instant messaging systems).
5. The County and its Shared IT Services Partners may use software that allows it to monitor messages, files, or other information that is entered into, received by, sent, or viewed on County and its Shared IT Services Partners' networks. By using County and its Shared IT Services Partners' equipment or the Internet access provided by it, users consent to the monitoring of all network and information systems.

III. Acceptable Use:

Personal or incidental use is authorized for limited purposes and will be subject to the following guidelines:

1. The use must not constitute a conflict of interest. Personal business or use for personal gain constitutes a conflict of interest.
2. Personal use is on personal time (hours not charged to us) and must not interfere with our business or normal work activities, and not adversely affect performance of the employee, surrounding employees, the organization, or business functions.
3. Illegal, obscene, pornographic, or offensive material must not be accessed, viewed, downloaded, or sent.
4. Any access that could result in significant incremental cost, such as noticeable additional electronic mail traffic, large non-business-related file transfers, and the like are not permitted.
5. Use must not involve any illegal or unethical activity (e.g., gambling, Warez sites containing pirated software, movies, games, or illegal hacking/cracking tools).
6. Transmitting or sending sensitive or proprietary information, including software applications or personal information, to unauthorized persons or organizations is prohibited. Authorization for any transmission of personally identifiable information ("PII") must be approved by a supervisor prior to transmission and done using authorized protocols (e.g. encryption, VPN, SSL).
7. Downloading or sending unapproved software, computer viruses, malicious code, or any unauthorized attempts to access another person's data or County and its Shared IT Services Partners' intranet are prohibited.
8. The addition of any hardware that would allow additional access to the Internet is prohibited.

9. Users may not download software from any outside systems without permission from the Department of Information Technology. Users should not use any externally provided software without first getting approval from Information Technology. Users should not download unapproved or unauthorized software from the Internet. Users are responsible for determining the sensitivity and need for further encryption to secure County and its Shared IT Services Partners confidential or sensitive information prior to posting, transmitting or sending it via the Internet. If unsure, the user is responsible for contacting Department of Information Technology or the County Attorney's Office for assistance.
10. County and its Shared IT Services Partners' privacy policy should be posted on all official County and its Shared IT Services Partners' websites to ensure that customers and clients are aware of our desire to maintain and protect the privacy of this data.
11. County and its Shared IT Services Partners' websites or web servers are not to be used for posting non-business-related data or for the illegal distribution of data, such as software, games, movies, code or other inappropriate data.

IV. Management and Maintenance Information Technology Controls:

The County Director of Information Technology shall be designated as the IT Administrator of the County and its Shared IT Services Partners' computer technology data systems. To minimize the County and its Shared IT Services Partners' threat of cyber liability exposures, the Department of Information Technology shall be responsible for the following controls:

1. Providing reports to the County Administrator and County Risk and Safety Committee on the status of the County's Information Technology Programming including, but not limited to cyber incidents, threats, and security protocols pertaining to the County's computer technology data systems on a regular recurring basis.
2. Immediately reporting any cyber incidents that may compromise County business data systems and operations to the County Administrator and the County Attorney.
3. Restricting authorization of the County's Information Technology Administrator privileges to senior management within its department.
4. Restricting the allocation of administrator privileges to specific equipment or applications that are aligned with departmental responsibilities. If a Department Head and/or their designee(s) requires wider privileges, to perform a specific task, allowing that privilege only for a limited time.
5. Requirements should be established to specify that the administrator passwords within the Department of Information Technology are more complex and changed more frequently in recognition of their responsibility. Administrator passwords should also be different than their user passwords.
6. Department of Information Technology Administrators shall maintain separate user accounts for their daily use and their administrator specific work. They should not be allowed to access the Internet or email from their privileged administrator accounts.
7. If services are outsourced to third parties, the Director of Information Technology shall be responsible for addressing the proper protection and control for third party administrative access and hold third-party providers accountable and professionally liable for their services including, but not limited to:

    a. Third parties should be restricted from using the same administrative passwords at multiple client locations because this can put your network at risk if the password is compromised at one of the other client locations.
    b. Requiring two-factor authentication for all third-party or remote administrators to gain access should be considered.

The Department of Information Technology shall be responsible for the management and maintenance of County computer systems including, but not limited to official County and its Shared IT Services Partners websites and social media; server rooms; computer hardware and software vendor relationships; security

access controls for County and its Shared IT Services Partners maintained security systems; internet-based communication systems; and County contracted shared service agreements.

V. Specialized Cyber Industry Procedures as Applicable

The County and/or its Shared IT Services Partners may use the following technology within their business operations. The terms and conditions that follow are the minimum standards required by the insurance industry for cyber liability coverage:

1. **Biometrics:** The County and its Shared IT Services Partners may use a timekeeping system that uses finger or hand-scanning technology for identification for its payroll processing and issuing paychecks. These timekeeping systems convert a scan of an employee's fingerprint, and/or fingertip ("finger scan") into an encrypted mathematical representation within a secure vendor data program. This technology does not collect and store fingerprints, nor does it retain fingertip images. This data is maintained, and managed by a contracted vendor who manages and troubleshoots payroll under the guidelines established by the County and/or its Shared IT Services Partners. The following general terms and conditions shall apply to the County and/or Shared Services use of this technology for payroll purposes:

    a. Consent: Employees required to use finger-scanners included in the timekeeping system as a condition of employment shall consent to the collection of the finger-scan mathematical representation by the payroll system and agree to provide consent at the time of initial fingerprint scan enrollment which provides a scan timekeeping device notice and provides the opportunity for consent. The announcement and consent are stated as follows:
    "I intend and agree to use my employer's timeclock devices with a finger sensor for timekeeping and attendance. By clicking 'Accept' below I understand, agree and voluntarily consent to the following:

    - *The sensor uses data from my finger scan from which it will create a unique finger template that is securely stored in the sensor and my employer's timekeeping database.*
    - *Templates may be considered biometric data.*
    - *My employer is responsible for providing all requisite notices and policies relating to the use of my personal information, including but not limited to providing a description of the data usage and security.*
    - *Policies provided by my employer regarding biometric data retention and destruction will apply. The timekeeping vendor will be responsible for permanently destroying my finger template when my employer deletes my data.*
    - *My consent applies to each use of the sensor, including past and future use.*
    - *The timekeeping vendor processes personal information on behalf of my employer for payroll purposes.*
    - *I can contact my employer about my rights that I have in connection with my personal information, including any right to withdraw consent.*

    Clicking 'Accept' is my signature and voluntary consent (if permissible by applicable law) to the collection, capture, storage, access to use, possession, dissemination, disclosure, re-disclosure, and hosting of any biometric data by my employer, and y employer's service provider (timekeeping vendor) and its affiliates, vendors, subsidiaries, or related companies and any of their subcontractors, resellers, or successors, consistent with my employer's timekeeping policy as applicable. I acknowledge that I can view and print a copy of this notice. ACCEPT or DECLINE."

    b. Disclosure: The County and its Shared IT Services Partners agree to not disclose, redisclose or disseminate the saved encrypted mathematical representation to anyone other than its payroll

vendor and any other vendors that maintain, fix, update or troubleshoot the timekeeping system for the purposes identified above without and/or unless:

i. First obtaining written employee consent to such disclosure or dissemination;
ii. The disclosure or re-disclosure completes a financial transaction requested or authorized by the employee;
c. Disclosure or re-disclosure is required by state or federal law or municipal ordinance; or
d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

The County and its Shared IT Services Partners shall not sell, lease, trade, or otherwise profit from the saved encrypted mathematical representation; however, the County and its Shared IT Services Partners may pay its payroll vendor for timekeeping and payroll products or services utilized by the County and its Shared IT Services Partners. The County and its Shared IT Services Partners may also pay a vendor to maintain, fix, update or troubleshoot the time clock.

c. Storage, Transmission, and Protection: The County and its Shared IT Services Partners and their respective vendors shall use a reasonable standard of care to store, transmit and protect from disclosure the saved encrypted mathematical representation. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the County and its Shared IT Services Partners stores, transmits, and protects from disclosure confidential and sensitive information, such as account numbers, PINs, driver's license numbers and social security numbers.

2. **Electronic Mail and/or Instant Message Use:** Policies and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Users are prohibited from creating or sending electronic mail:

a. that may be considered offensive or harassing, or that may contribute to a hostile environment;
b. that contains profanity, obscenities, or derogatory remarks;
c. that constitutes chain letters or spam;
d. to solicit or sell products or services that are unrelated to our business; or
e. to distract, intimidate or harass anyone, or to disrupt the workplace.

Users are instructed to use caution when opening electronic mail and attachments from unknown senders because these pieces of electronic mail and attachments may contain viruses, root kits, spyware or malware that can put our system and sensitive information at risk.

3. **Collaborative Software:** The Department of Information Technology shall be responsible for the approval and installation of collaborative software systems for County and its Shared IT Services Partners operations at the requests of County and its Shared IT Services Partners Department Heads and/or their designee(s). Once collaborative software approval is granted, County and its Shared IT Services Partners' computer users shall be responsible for the following:

a. Acceptable Use and Security:
   i. Not downloading, installing, or using unauthorized software on County and its Shared IT Services Partners equipment unless approval is first obtained from the County Department of Information Technology.
   ii. Protect sensitive and confidential information in accordance with federal and state laws.
   iii. Adhere to security measures by using strong passwords for accessing files or any content, and follow any document expiry or other risk mitigation rules.
   iv. Prohibit sending unsolicited messages, spam, or engaging in any form of harassment through communication tools.
b. Licensing and Copyright Including Software and Intellectual Property:

i. Respect all copyright and licensing agreements and not share or use copyrighted material illegally.

c. User Responsibilities:
   i. Use collaborative tools primarily for approved work-related purposes.
   ii. Not perform any action that compromises the performance or security of County Information Technology resources.

County and its Shared IT Services Partners Departments shall be responsible for their own cost of the installation, licensing and ongoing maintenance of any collaborative software installed within departmental computers.

4. **Multi-factor Authorization:** Multi-factor Authorization (MFA) is a security process whereby users must provide at least two different authentication factors to verify their identities and access their accounts. The County Department of Information Technology shall be responsible for the provision of MFA to County and its Shared IT Services Partners computer users. This process ensures better protection of both a user's personal information, credentials, and other assets, while also improving the security around the resources the user can access. The following MFA terms and conditions shall apply:

   a. All individuals shall be required to engage in one additional step beyond the normal login process to access County and its Shared IT Services Partners resources using County and its Shared IT Services Partners owned and/or maintained computer hardware not directly connected to the County and its Shared IT Services Partners Computer infrastructure.
   b. MFA shall be required for all externally exposed enterprise or third-party applications, where supported.
   c. MFA shall be required for remote network access.
   d. MFA shall be required for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.
   e. Responsibilities of all County and its Shared IT Services Partners sponsored computer users include, but are not limited to:
      i. It shall be the user's responsibility to promptly report compromised credentials to the Information Technology Team.
      ii. It shall be the user's responsibility to promptly report a lost or stolen MFA device to the Information Technology Team.
   f. Exemptions to these MFA requirements include those situations in which a member of the County and its Shared IT Services Partners community have a legitimate need to utilize technology resources outside the scope of this policy. The Information Technology Team may approve, in advance, exception requests based on balancing the benefit versus the risk to the County and its Shared IT Services Partners.

5. **Social Media:** The County and its Shared IT Services Partners support self-expression, including the right to express oneself to others via Internet blogs, social web pages, posting on open forums, or speaking during public events. Users may not use social networking sites while working unless authorized by their supervisor and the information posted pertains to County operations. Some points that the County and its Shared IT Services Partners want users to consider when writing or expressing themselves publicly:

   a. Conduct themselves in a professional and businesslike manner, even if the communication is personal in nature.
   b. Do not reference or discuss the County and its Shared IT Services Partners' suppliers, vendors, customers, associates, contractors, potential business relationships or opportunities, competitors, and/or any entity that the County and its Shared IT Services Partners do business with, or anything

that might adversely impact on the County and its Shared IT Services Partners' business relationships.

c. Do not make statements about the County and its Shared IT Services Partners' financial performance.

d. When users are participating in social networking sites, users must be transparent that their thoughts are their own. Unless the County and its Shared IT Services Partners officially designate the user, in writing, to speak or write for the County and/or its Shared IT Services Partners, users should never state that they write or speak on behalf of the County and its Shared IT Services Partners. They should never represent that their viewpoints may or may not be the same as the County and its Shared IT Services Partners, and users should make this clear to those reading or listening to their points of view. Users may consider a disclaimer to this effect, but note that it may not excuse improper or illegal conduct.

e. Do not disclose private, internal-use only, copyrighted, or confidential information belonging to the County and its Shared IT Services Partners or third parties, including employees, associates, suppliers, vendors, competitors, customers, or any other person or entity that associates or do business with the County and/or its Shared IT Services Partners. Such information includes personally identifying information (such as telephone numbers, Social Security numbers, credit or debit card numbers, or financial account numbers). Users should also not mention customers, vendors, potential business relationships or opportunities, or competitors in their social media activity. Users should use common sense and courtesy and should follow strictly the County and/or its Shared IT Services Partners' policy on preserving confidential information.

f. For social networking sites such as LinkedIn where personal and professional references are the focus: If users are representing themselves as a County and its Shared IT Services Partners employee, users may not provide professional references about any current or former employee, contractor, vendor, or contingent worker.

g. What users write or say, and how users write or say something, is up to each user. However, the County and its Shared IT Services Partners hereby provide notice that they reserve the right to read what users write or say publicly and make a determination if it meets the professional standards of or damages the County and/or its Shared IT Services Partners. Written or stated comments that may be construed as being harmful or damaging to the County and its Shared IT Services Partners or to its employees, associates, suppliers, vendors, customers, or any other person or entity that associates or does business with the County and its Shared IT Services Partners may lead to immediate termination. This provision does not in any way restrict users' right to engage in protected activity under Section 7 of the National Labor Relations Act.

h. Do not use vulgar, obscene, offensive, threatening, harassing, or defamatory language. Offensive language or content would include, but is not limited to, discrimination, harassment, or hostility on account of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic. Offensive language or content also includes soliciting sex or otherwise violating the laws regarding minors and their protection. Users that violate child protection laws, including solicitation of sex from minors, or posting of illegal pornographic material, will be subject to discipline including, but not limited to, termination.

Social media can be a beneficial tool for government agencies that wish to communicate with the public about their activities, such as events, programs, staffing changes and more. This type of activity, when undertaken correctly, can be a positive, educational outlet for our agencies. However, there are a number of details regarding Open Records Laws, court cases about censorship and more that apply to government-operated social media accounts that those who operate government social media must be cognizant of. In light of these factors, a Warren County employee who wishes to start a social media presence in the name of a Warren County agency or entity should contact the Director of Public Affairs beforehand to discuss the applicable rules and regulations. In the same circumstance, employees of

Shared IT Services Partners should contact their entity's government authority to determine how the Shared IT Service Partner wishes to manage their public entity's social media messages.

VI. Electronic Device Security Measures:

Employees and Personal Device Users shall abide by the terms and conditions of the County's Computer Use Policy and protect the County and its Shared IT Services Partners against cyber-attack by:

1. Avoiding opening emails or attachments from an unknown, suspicious, or untrustworthy source, especially when the content is not adequately explained. All unexpected content from a trusted source should be verified with that source prior to opening. Verification can be conducted by sending a separate follow-up email (not using the "reply" function), texting the alleged sender, or calling to validate that the email is from the correct source.
2. Being suspicious of clickbait headlines, which may be used to get employees to click on a link to go to a certain webpage, or malicious links. For example, if the domain of the link to which an employee is being directed does not match the purported company domain, then the link is fake.
3. Being suspicious of emails creating a false sense of urgency or quick response. For example, emails that warn employees of their account being closed or suspended unless immediate action is taken likely constitute a phishing attack.
4. Checking email and names of people they receive a message from to ensure they are legitimate.
5. Looking for inconsistencies or giveaways in emails. For example, grammar mistakes, capital letters, excessive number of explanation marks may all be indicators of a phishing scam.
6. Never giving out account passwords or County and its Shared IT Services Partners credentials by email.
7. Contacting the County Department of Information Technology if a questionable email is received that may jeopardize the integrity of the County and/or Shared IT Services Partners' computer systems.

VII. Employee Awareness and Training:

The County Risk and Safety Committee shall work with the Department of Information Technology for the provision of cyber security training on an annual and ongoing basis. The County and Shared IT Services Partners shall provide the financial support necessary to provide the recommended education and training in support of the County's Cyber Liability Programming. The Department of Information Technology shall be responsible for providing the County and its Shared IT Services Partners with continuous, hands-on employee training on how to detect email phishing scams and other cyber technology threats to County and its Shared IT Services Partners' computer systems. Such training shall regularly inform County and its Shared IT Services Partners employees, interns and volunteers about new scam emails or viruses and ways to combat them. The Department of Information Technology shall periodically send out fake phishing emails to test employees' knowledge and awareness of phishing scams.

VIII. Phishing Prevention and Reporting:

"Phishing" is a cybercrime in which a target or targets are contacted by someone posing as a legitimate institution or person to lure individuals into providing confidential information, such as County Sensitive Information, that will be used for unlawful and malicious purposes. The purpose of this policy is to outline guidelines and processes for the identification, prevention, and reporting of phishing scams, which will help to preserve the security of the County of Warren's data and technology infrastructure.

1. Email Security Measures to Prevent Phishing Attacks:

   To protect the County against phishing attacks via email, employees shall be educated to:

a. Avoid opening emails or attachments from an unknown, suspicious, or untrustworthy source, especially when the content is not adequately explained. All unexpected content from a trusted source should be verified with that source prior to opening. Verification can be conducted by sending a separate follow-up email (not using the "reply" function), texting the alleged sender, or calling to validate that the email is from the correct source.
b. Be suspicious of clickbait headlines, which may be used to get employees to click on a link to go to a certain webpage, or malicious links. For example, if the domain of the link to which an employee is being directed does not match the purported company domain, then the link is fake.
c. Be suspicious of emails creating a false sense of urgency or quick response. For example, emails that warn employees of their account being closed or suspended unless immediate action is taken likely constitute a phishing attack.
d. Check email and names of people they receive a message from to ensure they are legitimate.
e. Look for inconsistencies or giveaways in emails. For example, grammar mistakes, capital letters, excessive number of explanation marks may all be indicators of a phishing scam.
f. Never give out account passwords or County credentials by email. The County, or any credible website, shall not require you to share such information via email.
g. If an Employee is not sure if an email they received is safe, the employee shall refer to the IT Help Desk and await further instruction.
h. Comply with all other applicable policies, including, but not limited to, the County's Computer Use Policies.

2. Phishing Prevention:

To prevent the County's domain from being used in phishing scams, the Department of Information Technology shall, in addition to other security procedures required by other County policies, be responsible for:

a. Implementing domain level email authentications so that receiving mail servers can verify that a message that claims to be from the County actually came from a domain authorized by the County.
b. Implementing Domain Message Authentication Reporting and Conformance ("DMARC") which, among other things, will enable the County to:
    i. gather intelligence on how phishers and other scam artists may be misusing County domains, and
    ii. instruct receiving email servers on how to treat unauthenticated messages that claim to be from the County's domain.
c. Installing antivirus solutions, schedule signature updates, and require multi-step authentication to prevent hackers from gaining access to County assets.

3. Reporting a Phishing Attack:

a. Employees must report perceived attacks, suspicious emails or phishing attempts as soon as possible to the Department of Information Technology.
b. The Department of Information Technology shall be responsible for promptly investigating a reported phishing attack, resolving the issue, and notifying the County Administrator, the County Attorney (or Shared Services Corporate Counsel), and other County Employees of the status of the phishing attack and its remediation efforts, as appropriate.
b. Phishing attacks should be reported by forwarding the original phishing message, with full message headers, to the County Department of Information Technology Help Desk email.
c. The Department of Information Technology shall be responsible for providing cyber security incident information to users as soon as practicable..

IX. Vendor Management

Computer hardware and software vendors shall be required to adhere to the County and its Shared IT Services Partners' contractual terms and conditions as specified in ***"The County of Warren Exhibit F: Supplemental Terms and Conditions: Hardware, Software, Coding and Cloud Computing"*** herein attached as **Attachment B** to this policy.

X. Enforcement

The Director of Information Technology shall work with County officials and Shared IT Services Partners to enforce the terms and conditions of this Computer Use Policy to include, but not be limited to the following:

1. **Non-Compliance:** Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. The County reserves the right to advise appropriate authorities of any violation of the law as may be identified by the terms and conditions of this policy.
2. **Exceptions:** Any exception to this policy must be approved by Director of Information Technology in partnership with the County Attorney.
3. **User Acknowledgement:** The Department of Information Technology shall be responsible for ensuring that a user acknowledgement or a non-disclosure agreement has been signed by all users acknowledging this Acceptable Use Policy before providing access to County's sensitive computing resources.
4. **Compliance Measurement:** The Department of Information Technology shall verify compliance with this policy through various methods, including, for example, business tool reports and audits.

SCHEDULE A
Computer Use Policy Attachment A

ACKNOWLEDGEMENT OF COUNTY COMPUTER USE POLICY

I have received and reviewed a complete written copy of County of Warren's Computer Use Policy, effective _____, per Board of Supervisors Resolution No. _____ of 2026 (hereafter, "Computer Use Policy"). I fully understand and acknowledge the terms of this Computer Use Policy and shall abide by each any every requirement stated by the Computer Use 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 accessed by authorized County officers, employees or agents for use by County management.

I acknowledge and accept that violations of the Computer Use 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**

Please return this original signed form to the Department of Human Resources.

County Computer Use Policy Attachment B: Contract EXHIBIT F

Supplemental Terms & Conditions: Computer Hardware, Software, Coding, and Cloud Computing

County of Warren, NY **(Version 1.03 eff. 4/21/2025)**

The Contractor, for itself, it's assignees, and successors-in-interest (hereinafter collectively referred to as "the Contractor") acknowledge and agree that if this Agreement involves the purchasing of computer hardware, purchase or licensing of software, or cloud computing services, then the Contractor agrees and accepts at these supplemental terms and conditions are incorporated into the parties' Agreement:

1. **Definitions:**
   a. **Computer Hardware**: The physical components of a computer system, including both internal devices that work together to enable a computer to process information, store data, and communicate with the user.
   b. **Data Breach**: A security incident where unauthorized individuals access or disclose confidential or sensitive information caused by intentional hacking or accidental events.
   c. **Data Security**: Measures taken to protect digital information from unauthorized access, corruption or theft throughout the digital information's lifecycle.
   d. **Intellectual Property**: A creation of the mind such as inventions, literary works, artistic works, program coding or pictorial images to which one has legal rights to and for which one may apply for a patent, copyright or trademark.
   e. **Personal Data**: Information specific to an individual that may directly or indirectly identify them by an identification number, location data, physiological, genetic, mental, commercial, cultural or social identity.

2. **Responsibilities of the Parties (Hardware & Software)**: The Contractor shall work with the County's Information Technology staff to design and install hardware and/or software systems that are in conformance with County IT infrastructure and programming including data security protocols. The County shall take possession of the management and control of the product and/or services provided under this agreement upon the accepted completion of the project and shall assume full responsibility for the County's content maintenance and administration.

3. **Representations and Warranties.**
   a. **Contractor's Warranties.** The Contractor represents and warrants as follows:
      i. **Authority**. The Contractor has the full power, capacity and authority to enter into and perform this Agreement and to make the grant of rights contained herein, including without limitation, the right to license any ancillary or third party programs licensed to the County under this Agreement, and the Contractor's performance of this Agreement does not violate or conflict with any agreement to which the Contractor is a party; The Contractor further represents that there is no pending or threatened litigation that would have a material adverse impact on its performance under this Agreement;
      ii. **Conformance to Specifications**. All Services and Deliverables shall materially conform to the Specifications during the Term;
      iii. **Non-Infringement**. The Services and the Deliverables (excluding any of the County's Property) shall not infringe upon or violate the intellectual property rights of any third party;
      iv. **No Offshore Work**. The Contractor further warrants that all Services shall be performed and rendered within the continental United States. In particular, the Contractor warrants that it shall not transmit or make available any Confidential Information of the County, to include Personal Data, or County Property to any entity or individuals outside the continental United States;
      v. **Documentation; Material Diminution in Features**. The Documentation shall be complete and accurate so as to enable a reasonably skilled person to effectively use all of its features and functions without assistance from the Contractor and, on each date on which Contractor delivers it to the County, the Documentation is Contractor's most current version thereof; provided that, without the prior written approval of the County, in no event shall any Documentation reflect a material diminution in the form, features or functionality of the Services from that originally licensed under this Agreement, and, accordingly, the Contractor shall not change the form, features or functionality in any material adverse manner from that originally licensed under this Agreement;
      vi. **Assignment of Warranties**. The Contractor hereby assigns and agrees to deliver to the County all representations and warranties received by the Contractor from its third-party licensors and suppliers;
      vii. **Viruses and Destructive Code**. The Contractor shall use reasonable efforts to ensure the Services and Deliverables do not include or transmit any viruses, Trojan Horses, worms, spyware, or other similarly destructive or malicious code;
      viii. **Legal and Accreditation Requirements**. The Services currently comply with all other existing federal, state and local laws; and the Contractor shall provide the County with the functionality necessary for the County to comply with all new, amended, or otherwise modified laws, applicable to the Services at no additional charge to The County;

County Computer Use Policy Attachment B: Contract EXHIBIT F

Supplemental Terms & Conditions: Computer Hardware, Software, Coding, and Cloud Computing

County of Warren, NY **(Version 1.03 eff. 4/21/2025)**

ix. **Compliance with Privacy Policy, Laws, and Regulations**. The Contractor shall comply with all applicable laws and regulations in its performance of this Agreement, including, but not limited to, all local, state, federal, and international privacy, confidentiality, consumer protection, advertising, electronic mail, data security, data destruction, and other similar laws, rules, and regulations, whether in effect now or in the future;

x. **Known Performance Issues**. There is no existing pattern or repetition of customer complaints regarding the Services and Deliverables, including functionality or performance issues, and that the Contractor's engineers have not currently identified any repeating adverse impact on the Services or Deliverables, including functionality or performance, for which the root cause is believed to be a flaw or defect in the Services or Deliverables. The foregoing warranty shall not extend to any specifications provided by the County;

xi. **Computer Hardware**. Contractor warrants that, under normal use and service, the Computer Hardware shall be free from defects in material and workmanship for a period of sixty (60) days after delivery and acceptance of the Computer Hardware to the County. The foregoing warranty shall not apply to consumables or portions of the Computer Hardware that are expendable by their nature;

i. If the Computer Hardware fails to meet the warranties of Section xi and the County gives Contractor written notice thereof during the warranty period, the Contractor may correct the failure by repair, replacement, or adjustment; or at the County's option and sole discretion, the Contractor may take back the computer hardware and return the purchase price to the County within thirty (30) after the County provides the Contractor written notice of the defect, whereupon the Contractor shall have no further obligation to the County;

ii. The County shall be solely responsible for the selection, use, efficiency, and suitability of the Computer Hardware; and

iii. The Contractor shall not be liable to County for the warranty provisions of this Section xi, if: Modifications are made to the Computer Hardware by other than the Contractor; Attachments, features, or devices are employed on the Computer Hardware that are not supplied by the Contractor and are not approved in writing by the Contractor; Other than the current version of the operating system software available from the Contractor is used on the Computer Hardware; or the computer hardware is subject to misuse or abuse.

b. **The County's Warranty.** The County represents and warrants that the County shall have the full power to enter into and perform this Agreement and to make the grant of rights contained herein, and the County's performance of this Agreement shall not violate or conflict with any agreement to which The County is a party.

4. **The County's Property.** "The County's Property" means any property or intellectual property provided by the County, or its agents, to the Contractor for use in connection with the Services, including, but not limited to, any data, images, programming, computer code, photographs, illustrations, graphics, audio clips, video clips, or text. The County grants the County a non-exclusive, non-transferable, non-sublicensable, terminable at-will license to use the County's Property solely for the County's benefit in performing the Services. Upon the County's written request or upon expiration of this Agreement or termination of this Agreement for any reason, the foregoing license shall immediately terminate. All County Property shall be deemed County Confidential Information.

5. **Confidentiality.**

a. **Confidential Information.** Except as provided in Exhibit B, section 19,and Exhibit E (Standard Business Associate Agreement), each Party agrees that all information supplied by one Party and its affiliates and agents (collectively, the "**Disclosing Party**") to the other ("**Receiving Party**") including, without limitation, (i) source code, prices, trade secrets, databases, designs and techniques, engine protocols, models, displays and manuals, and the selection, coordination, and arrangement of the contents of such materials; and (ii) any unpublished information concerning research activities and plans, customers, marketing or sales plans, sales forecasts or results of marketing efforts, pricing or pricing strategies, costs, operational techniques, strategic plans, information relating to the County's customers, business partners, and personnel, Personal Data (as defined below), and unpublished financial information, including information concerning revenues, profits and profit margins will be deemed confidential and proprietary to the Disclosing Party, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential" or "proprietary" ("**Confidential Information**"), provided, however, that Work Product assigned to the County pursuant to this Agreement shall be Confidential Information of the County.

b. **Exclusions.** Confidential Information will not include any information or material, or any element thereof, whether or not such information or material is Confidential Information for the purposes of this Agreement, to the extent any such information or material, or any element thereof: (a) has previously become or is generally known, unless it has become generally known through a breach of this Agreement or a similar confidentiality or non-disclosure

County Computer Use Policy Attachment B: Contract EXHIBIT F

Supplemental Terms & Conditions: Computer Hardware, Software, Coding, and Cloud Computing

County of Warren, NY **(Version 1.03 eff. 4/21/2025)**

agreement, obligation or duty; (b) was already rightfully known to the Receiving Party prior to being disclosed by or obtained from the Disclosing Party as evidenced by written records kept in the ordinary course of business or by proof of actual use by the Receiving Party; (c) has been or is hereafter rightfully received by the Receiving Party from a third person (other than the Disclosing Party) without restriction or disclosure and without breach of a duty of confidentiality to the Disclosing Party; or (d) has been independently developed by the Receiving Party without access to Confidential Information of the Disclosing Party. It will be presumed that any Confidential Information in a Receiving Party's possession is not within exceptions (b), (c) or (d) above, and the burden will be upon the Receiving Party to prove otherwise by records and documentation.

c. **Treatment of Confidential Information.** Each Party recognizes the importance of the other's Confidential Information. In particular, each Party recognizes and agrees that the Confidential Information of the other is critical to their respective businesses and that neither Party would enter into this Agreement without assurance that such information and the value thereof will be protected as provided in this Section 3 and elsewhere in this Agreement. Accordingly, each Party agrees as follows: (a) the Receiving Party will hold any and all Confidential Information it obtains in strictest confidence and will use and permit use of Confidential Information solely for the purposes of this Agreement. Without limiting the foregoing, the Receiving Party shall use at least the same degree of care to avoid disclosure or use of this Confidential Information as the Receiving Party employs with respect to its own Confidential Information of a like importance, which shall not be less than the standard of care imposed by applicable laws and regulations relating to the protection of such information and, in the absence of any legally imposed standard of care, the standard shall be that of a reasonable person under the circumstances; (b) the Receiving Party may disclose or provide access to its responsible employees who have a need to know and may make copies of Confidential Information only to the extent reasonably necessary to carry out its obligations hereunder; and (c) the Receiving Party currently has, and for so long as it possesses Confidential Information of the Disclosing Party, it will maintain in effect and enforce, rules and policies to protect against access to or use or disclosure of Confidential Information other than in accordance with this Agreement, including without limitation written instruction to any agreements with employees and agents who are bound by an obligation of confidentiality no less restrictive than set forth in this Agreement to ensure that such employees and agents protect the confidentiality of Confidential Information. The Receiving Party will instruct and require its employees and agents not to disclose Confidential Information to third parties, including without limitation customers, subcontractors or consultants, without the Disclosing Party's prior written consent; and will notify the Disclosing Party immediately of any unauthorized disclosure or use, and will cooperate with the Disclosing Party to protect all proprietary rights in and ownership of its Confidential Information.

d. **Personal Data.** In connection with this Agreement and performance of the Services, The Contractor may be provided or obtain, from the County or otherwise, Personal Data, as defined below, pertaining to the County's personnel, directors and officers, agents, subcontractors, investors, and customers and (ii) may need to process such Personal Data and/or transfer it, all subject to the restrictions set forth in this Agreement and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the Services. For purposes of this Agreement, "**Personal Data**" shall mean any information relating to an identified or identifiable individual. For the avoidance of doubt, Personal Data shall include, but not be limited to, all "nonpublic personal information," as defined under the Gramm-Leach-Bliley Act (15 United States Code ("**U.S.C.**") § 6801 et seq.), "protected health information" as defined under the Health and Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d), "cardholder information" under the Payment Card Industry ("**PCI**") Data Security Standard, and "Personal Data" as that term is defined in EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data. "Process" or "Processing" shall mean any operation or set of operations performed upon the Personal Data, whether or not by automatic means, including collection, recording, organization, use, transfer, disclosure, storage, manipulation, combination and deletion of Personal Data.

e. **Treatment of Personal Data.** Without limiting any other warranty or obligation specified in this Agreement, and in particular the confidentiality provisions of this section, during the Term and thereafter in perpetuity, The Contractor will not gather, store, log, archive, use or otherwise retain any Personal Data in any manner and will not disclose, distribute, sell, share, rent or otherwise transfer any Personal Data to any third party, except as expressly required to perform its obligations under this Agreement or as The Contractor may be expressly directed in advance in writing by the County. The Contractor represents, covenants, and warrants that the Contractor will use Personal Data only in compliance with (i) this Agreement, (ii) the County's current privacy policy, Warren County Policy for Red Flags Identity Theft Prevention, Resolution 485 of 2024, effective December 20, 2024, available at www. Warrencountyny.gov/MMA, and (iii) all applicable local,

County Computer Use Policy Attachment B: Contract EXHIBIT F

Supplemental Terms & Conditions:
Computer Hardware, Software, Coding, and Cloud Computing

County of Warren, NY **(Version 1.03 eff. 4/21/2025)**

state, federal, and international laws and regulations (including but not limited to all current and future laws and regulations relating to privacy, confidentiality, consumer protection, advertising, electronic mail, data security, data destruction, and other similar laws, rules, and regulations). The Contractor will immediately notify the County of any actual or suspected breach of confidentiality or security with regard to Personal Data. At no additional charge or cost to the County, The Contractor will fully cooperate with the County in investigating the breach, including, but not limited to, the provision of system, application, and access logs, conducting forensics reviews of relevant systems, imaging relevant media, and making personnel available for interview. On notice of any actual or suspected breach, the Contractor will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the breach in accordance with industry best practices. In the event any breach of security or confidentiality with regard to Personal Data by the Contractor or its agents requires notification to an individual under any law, rule, or regulation, the County will have sole control over the timing, content, and method of notification and the Contractor will promptly reimburse the County for all costs and expenses incurred as a result of the breach, including but not limited to, notice, print and mailing costs, and the costs of obtaining credit monitoring services and identity theft insurance for the individuals whose Personal Data was or may have been compromised. At no charge to the County, The Contractor will cooperate with the County and any regulator or other governmental entity having jurisdiction over the County or the Personal Data relating to the Contractor's performance of this Agreement and possession and use of the Personal Data.

f. **Retention of Personal Data.** The Contractor will not retain any Personal Data for any period longer than necessary for the Contractor to fulfill its obligations under this Agreement. As soon as the Contractor no longer needs to retain such Personal Data in order to perform its duties under this Agreement, the Contractor will promptly return or destroy or erase all originals and copies of such Personal Data.

g. **Compelled Disclosures.** To the extent required by applicable law or by lawful order or requirement of a court or governmental authority having competent jurisdiction over the Receiving Party, the Receiving Party may disclose Confidential Information in accordance with such law or order or requirement, subject to the following conditions: as soon as possible after becoming aware of such law, order or requirement and prior to disclosing Confidential Information pursuant thereto, the Receiving Party will so notify the Disclosing Party in writing and, if possible, the Receiving Party will provide the Disclosing Party notice not less than five (5) business days prior to the required disclosure. The Receiving Party will use reasonable efforts not to release Confidential Information pending the outcome of any measures taken by the Disclosing Party to contest, otherwise oppose or seek to limit such disclosure by the Receiving Party and any subsequent disclosure or use of Confidential Information that may result from such disclosure. The Receiving Party will cooperate with and provide assistance to the Disclosing Party regarding such measures. Notwithstanding any such compelled disclosure by the Receiving Party, such compelled disclosure will not otherwise affect the Receiving Party's obligations hereunder with respect to Confidential Information so disclosed.

h. **Return of Confidential Information.** On the County's written request or upon expiration or termination of this Agreement for any reason, the Contractor will promptly: (a) return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing the County's Confidential Information; and (b) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by the Contractor, prepared under its direction, or at its request from the documents and materials referred to in subparagraph (a), and provide a notarized written statement to the County certifying that all documents and materials referred to in subparagraphs (a) and (b) have been delivered to the County or destroyed, as requested by the County. On termination or expiration of this Agreement, the County shall return or destroy all The Contractor Confidential Information (excluding items licensed to the County hereunder or that are required for use of the Deliverables), at The Contractor's option.

i. **Non-Exclusive Equitable Remedy.** Each Party acknowledges and agrees that due to the unique nature of Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach or threatened breach may allow a Party or third parties to unfairly compete with the other Party resulting in irreparable harm to such Party, and therefore, that upon any such breach or any threat thereof, each Party will be entitled to appropriate equitable remedies and may seek and obtain injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss or posting of a bond or other security, in addition to whatever remedies either of them might have at law or equity. Any breach of this Section 3 will constitute a material breach of this Agreement and be grounds for immediate termination of this Agreement in the exclusive discretion of the non-breaching Party.

County Computer Use Policy Attachment B: Contract EXHIBIT F

Supplemental Terms & Conditions: Computer Hardware, Software, Coding, and Cloud Computing

County of Warren, NY **(Version 1.03 eff. 4/21/2025)**

6. **Data Security**: The Contractor will maintain and enforce safety and physical security procedures with respect to its access, use, and possession of the County's Confidential Information, including Personal Data, that are (a) at least equal to industry standards for such types of locations, and (b) which provide reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of such information. Without limiting the generality of the foregoing, The Contractor will take all reasonable measures to secure and defend its location and equipment against "hackers" and others who may seek, without authorization, to modify or access the Contractor's systems or the information found therein. The Contractor will periodically test its systems for potential areas where security could be breached. The Contractor will immediately report to the County any breaches of security or unauthorized access to the County's Confidential Information, including Personal Data, that the Contractor detects or becomes aware of. The Contractor will use diligent efforts to remedy such breach of security or unauthorized access in a timely manner and deliver to the County a root cause assessment and future incident mitigation plan with regard to any breach of security or unauthorized access affecting the Confidential Information, including Personal Data. The Contractor shall provide the County all written details regarding the Contractor's internal investigation regarding any security breach. Upon the County's request, the Contractor will provide a second more in-depth investigation and results of findings. The Contractor agrees not to notify any regulatory authority nor any customer or consumer, on behalf of the County, unless the County specifically requests in writing that the Contractor do so. The Contractor and the County will work together to formulate a plan to rectify all security breaches. At a minimum, the Contractor represents, promises and warrants that it shall adhere to the global data protection and privacy laws and their security protocols including, but not limited to the following: General Data Protection Regulation (GDPR); Health Insurance Portability and Accountability Act (HIPAA); Gramm-Leach-Bliley Act (GLBA); and Federal Information Security Management Act (FISMA). The County in the event of a security breach due to the negligence, malicious actions, omissions, or misconduct of the Contractor, the Contractor, as the data custodian of the security breach, will comply and be financially responsible for all remediation efforts as required by applicable federal and state law suffered by the County in the provision of the product and/or services provided.

7. **Intellectual Property**: Intellectual property in the hardware and/or software or other works created or licensed by the Contractor, including all software source code, documents, and materials used in performing services will remain the property of the Contractor. Contractor property specifically excludes County content. The County shall not license, sublicense, sell, resell, reproduce, transfer, assign, distribute or otherwise commercially exploit or make available to any third party any Contractor property in any way, except as specifically provided in Exhibit A's Scope of Work.

The Contractor grants the County a nontransferable, nontransferable, nonexclusive, non-assignable license to access and use Contractor property associated with any valid and effective Scope of Work provided in Exhibit A for the term of the agreement stated. The Contractor agrees to provide periodic updates to the product and service provided in accordance with County IT standards.

8. **Contractor Support**: The Contractor shall provide support for the product and/or services stated in Exhibit A of this agreement. The County as a government agency reserves the right to obtain emergency services, as needed, and at the agreed upon price structure outlined within Exhibit A, if the County identifies the support for the need for the product and/or services to be an emergency as defined by section 103(4) of the General Municipal Law

9. **Termination Assistance Services.** Upon the expiration of this Agreement or its termination by either Party for any reason, including the breach of this Agreement by the other Party, the rights of the County shall in any and all events be provided as set forth in this Section ("**Termination Assistance Services**"). Unless the Parties have specifically agreed upon a termination transition plan prior to the time of termination (the "**Termination Transition Plan**"), the rights of the County upon any termination shall be as set forth in this Section. If a Termination Transition Plan has been agreed to, then the rights of the County upon any expiration or termination of this Agreement shall be as set forth in the most recent approved Termination Transition Plan, and also as set forth in this Section. In the event of any inconsistency between this Section and the applicable Termination Transition Plan, this Section shall govern. If no Termination Transition Plan has been agreed to by the Parties at the time of any termination of this Agreement, then the Contractor shall continue to perform the services under the Agreement, at performance standards and service levels in effect at the time of termination or expiration, as well as the transition assistance services, which services shall be provided as set forth in this Section. The Contractor shall provide the County with all of the services and all of the transition services as provided in this Section and in the then most recent version

County Computer Use Policy Attachment B: Contract EXHIBIT F

Supplemental Terms & Conditions:
Computer Hardware, Software, Coding, and Cloud Computing

of the Termination Transition Plan, if any. The duty of the Contractor to provide such services shall be conditioned on the County continuing to comply with its obligations under the Agreement, including payment of all fees. The Contractor shall have no right to withhold or limit its performance or any of such transition services on the basis of any alleged breach of this Agreement by the County, other than a failure by the County to timely pay the amounts due hereunder during the transition period. The County shall have the right to seek specific performance of this Section in any court of competent jurisdiction and the Contractor hereby waives any defense that damages are an adequate remedy. Compliance with this Section by either Party shall not constitute a waiver or estoppel with regard to any rights or remedies available to the Parties. The Contractor will (i) meet with the County as soon as practicable after a notice of termination or notice of a decision to not extend this Agreement has been given, to discuss any potential modifications to the then most current Termination Transition Plan, if any, (ii) use all commercially reasonable efforts to assist the County effecting a transition of the services provided by the Contractor hereunder, in accordance with industry best practices, to the County or another vendor chosen by the County, and (iii) be compensated for all transition related services and costs by payment by the County in accordance with the rates set forth in this Agreement. The Contractor will provide transition services for a period defined in the Termination Transition Plan, if any, but in no event less than six (6) months following the expiration or termination of this Agreement. Thereafter, the Contractor shall provide extensions of transition support services as requested by the County in serial thirty (30) day extension terms for up to an additional six (6) months. The total period of transition support services, including all extensions provided for herein, shall not exceed twelve (12) months.

10. **Marketing:** The Contractor must receive prior written permission from the County before identifying the County, using any of its identifying information including logos and County specific services, and any of the product and/or services provided under Exhibit A of this agreement.