# Warren County Board of Superbisors

## RESOLUTION NO. 485 OF 2024

**RESOLUTION INTRODUCED BY SUPERVISORS WILD, DRISCOLL, MERLINO, MADAY, BEAN, ETU AND THOMAS**

**ADOPTING THE WARREN COUNTY POLICY FOR RED FLAGS IDENTITY THEFT PREVENTION**

WHEREAS, the County Attorney presented to the Personnel, Administration & Higher Education Committee a Warren County Policy for Red Flags Identity Theft Prevention, and

WHEREAS, the Personnel, Administration & Higher Education Committee has reviewed the Policy and has recommended that the same be advanced to the full Board of Supervisors for consideration, now, therefore, be it

RESOLVED, that the Warren County Policy for Red Flags Identity Theft Prevention, annexed hereto as Schedule "A," be and the same is hereby adopted as the official policy for Warren County.

## SCHEDULE "A"
## Policy and Program for Red Flags Identity Theft Prevention

### I. Policy Statement:

The Warren County Policy for Identify Theft Prevention (the "Policy") is hereby adopted by the Warren County Board of Supervisors (the "County") to help protect County officers, employees, residents, visitors, contractors, vendors and the County of Warren from physical and financial dangers and damages which result from the loss, theft or misuse of sensitive information, as more fully described by the Federal Trade Commission's Identity Theft Prevention Red Flags Rule. The Identity Theft Red Flags Rule ("Red Flags Rule") is a Federal Trade Commission (FTC) regulatory framework that requires organizations that access and store an individual's personal information to establish a written Identity Theft Program (ITPP) to identity and respond to potential incidents of identity theft. The Fair Credit Reporting Act's Identity Theft Rule and its subsequent updates are hereby adopted by the County of Warren to govern the safekeeping of personal information stored, maintained and accessed during County business operations in order to combat identity theft and related fraud.

### II. Purposes of Policy:

The purposes of the policy are to define sensitive information and its physical security when printed and when stored and transmitted in electronic communications. The goal of this policy is to enable the County to actively comply with state and federal regulations regarding identity theft within County workspaces and computer networks. The policy enables County officers and employees to protect existing customers, retirees, contractors, vendors and employees by reducing risk of identity fraud and minimizing the potential financial loss, physical damage, and reputational damage to the County and its operations as a result of fraudulent activity.

The policy will assist the County:

1. Identity risks that signify potentially fraudulent activity.
2. Detect risks when they occur.
3. Respond to risks to determine if fraudulent activity has occurred and to act accordingly if a breach of the County's data systems has occurred and/or fraud has been attempted or committed.
4. Update the Policy periodically, including reviewing covered areas and the risks identified as part of the programming set forth by the Policy.

In the event of any conflict between this policy and New York State licensing and vital records requirements, New York State laws and its requirements shall prevail.

### III. Definitions:

1. **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.
2. **Employee:** An individual employed by the County on a part-time or full-time basis, as well as volunteers and interns.

3. **Identity Theft:** Fraud committed or attempted using the identifying information of another person without their permission.
4. **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.
5. **Red Flag:** A pattern, practice or specific activity that indicates the possible occurrence of identity theft.
6. **Sensitive Information:** Any personal identifiable information collected by the County for a stated purpose in which the risk of identity theft is present.

## IV. Preventing Identity Theft Through Security of Data and Documents:

County personnel are encouraged to use common sense judgment in securing personal identifiably information. Any County document marked "Confidential" or "Privileged and Confidential" by an authorized County employee is not for public distribution, except as required by legal process or Freedom of Information Law.

Every County officer and employee shall sign an ***"Employee Confidentiality Agreement"*** for the County of Warren ***(Attachment A)***. New officers and employees to the Sheriff's Department will follow the guidelines of the Sheriff's Department Policies and Procedures respectively. All civilian and uniform employee confidentiality agreements will be kept on file in the employee's permanent personnel file.

### A. Sensitive Information Location Identification:

The County has identified the following locations where sensitive information is present: (this is a representative list and is not all inclusive of additional locations where confidential information may be present).

1. Planning and Economic Development: Loan, Grant and Assistance Applications;
2. Human Resources and Self-Insurance Departments: Payroll, Retiree, Employment, and Workers Compensation Records;
3. County Clerk's Office, including Birth Records; Death Records; Marriage Licenses;
4. Sheriff's Office;
5. Department of Social Services;
6. Department of Health Services;
7. County Attorney's Office;
8. County Public Defender's Office;
9. Information Technology Department/Computer Network Security.

### B. Guidelines for Securing Sensitive Information:

The following are guidelines for securing personal identifying information or sensitive information which every County employee shall follow and obey:

1. **Hard Copy Document Management:**

   a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use. Keys shall be stored in a secure location with access limited to those individual employees who require access.
   b. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised. A log containing the location of all County documents in storage will be kept by the Records Management Officer.
   c. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use and at the end of each business day.
   d. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
   e. When working papers containing sensitive information are discarded, they will be shredded by the employee discarding the materials. Documents considered municipal records, however may only be destroyed in accordance with Retention Schedule LGS-1 and with the written permission of the County's Records Management Officer. The Disposition sheet must also contain the signature of the department head/custodian of those records.
   f. Birth and death records are secured as mandated by the New York State Department of Health.
   g. Sheriff Department documents are secured per the Sheriff Department Policy and NYSPIN regulations.
   h. Vault doors must remain closed during business hours in County Offices. Combinations shall be changed periodically as needed and/or after an employee having the combination leaves employment.
   i. A request in writing by an employee for viewing of his/her permanent personnel file shall only be honored with verification of identity as prescribed in Section V of this policy **and in accordance with the "Freedom of Information Law" policy.** A record of the viewing and/or release of such documents evidencing the signature of both the County employee providing the information and the requesting party receiving the information shall be kept in the employee's permanent personnel file in accordance with the County's record retention policy and the NYS Retention Schedules.
   j. Requests for documents containing sensitive information shall only be honored with verification of identity as prescribed in Section V of this policy and to those individuals prescribed on the request form. A record of the release of such documents evidencing the signature of both the County employee providing the information and the requesting party receiving the information shall be kept by each department in accordance with the County's record retention policy and the NYS Retention Schedules.

2. **Electronic Document Management:**

   a. The County's e-mail system is a County-owned system. All e-mails sent and received within the County e-mail system are the property of the County, as more fully set forth by the Warren County **Computer Usage Policy**, approved by Resolution No. 144 of 2023. E-mails sent through the County e-mail system may be monitored under the provisions of the U.S.

Electronics Communication Privacy Act (ECPA) and Computer Usage Policy.

b. Access to the County's computer network is authorized and controlled by the Director of Information Technology. Access by an employee to the County's computer network, to include e-mail and stored data, is a privilege enjoyed by employees. No employee possesses any legal rights to access the County's computer network. To obtain access to the County's computer network, to include e-mail and stored data, employees must:
   i. Be classified by Civil Service as full-time, part-time, seasonal, or an intern.
   ii. Be granted access by the Director of Information Technology, or their designee no sooner than the employees' start date with access terminating no later than the last date of service with the County.
   iii. A signed "Acknowledgment of Warren County Computer Usage Policy" from the Computer Usage Policy must be obtained by the IT Department before access is granted. The agreement shall be filed in the employee's permanent personnel file. The level of computer access shall depend upon an employee's job requirements as defined by the appointing authority and Civil Service. Times of access shall only be permitted during normal work hours for work-related activities, or at other times as required by the employee's title.
   iv. A signed "Warren County Confidentiality Agreement," enclosed at Attachment "A."

c. All computers must be locked out when unattended and logged off of at the end of the workday. If this does not take place within a specified amount of time and lack of use of the workstation is detected, an administrative override will occur and the workstation shall be locked.

d. All employees must comply with the "Computer Usage Policy," found in Resolution No. 144 of 2023, and any future updates to the Computer Usage Policy.

e. All e-mails sent from the County of Warren must include the following statement:

   *"Confidentiality/Privilege Notice: This e-mail communication and any files transmitted with it contain privileged and confidential information from the County of Warren and are intended solely for the use of the individual(s) or entity to which it has been addressed. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any other action with respect to the contents of this message is strictly prohibited. If you have received this e-mail in error, please delete it and notify the sender by return e-mail. Thank you for your cooperation."*

f. Fax machines, copiers, printers, hard drives and other digital devices must have the storage device removed or securely erased prior to being removed from County premises.

g. Each County department that performs online financial transactions shall designate one computer for such departmental transactions. The designated computer shall be "white" listed preventing it from accessing any web site addresses that does not have a documented departmental business need.

h. All County computers shall be equipped with anti-malware software and or systems that feature automatic updates. New software and hardware patches shall be installed routinely.

i. The County shall maintain a cyber clock/black list and enforcement shall be on the network perimeter.

j. With the exception of publicly facing web interfaces, external access to any internal County network must be done with a County approved VPN.

k. Administrative passwords shall be periodically changed, including routers, firewalls, other

network equipment and software. Factory default passwords shall not be used on security equipment and systems.

l. When conducting financial transactions, the financial institution's web address must start with "https" not "http." The "s" indicates that the web site is secure, using a different method of communication than standard internet traffic. Users shall also confirm a valid SSL certificate prior to entering any information.

m. Links shall never be used to access a financial institution's site. E-mail and search engine links should not be trusted. Always type the financial institution's web address directly into the internet browser's address bar.

n. Users should learn what the financial institution's web site looks like and what questions are asked to verify identity. The slightest change of a web site in appearance, poor grammar, and/or additional security questions may signify a "man-in-the-middle" attack.

o. Credit card transactions shall be processed in compliance with the "Payment Card Industry Data Security Standard (PCI DSS).

p. Employees will not use County account passwords or similar passwords for any personal accounts unrelated to County operations. Employees when asked to choose passwords will not use a password or similar password to any passwords they use on personal non-County related accounts.

## V. Identification of Red Flags:

Red Flags are categorized into four separate classes: (1) Employee; (2) Management; (3) Public; and (4) Third Party. The County has identified some relevant Red Flags for each category, as follows:

1. Employee Red Flags may include, but are not limited to:

a. Lifestyle changes: expensive cars, jewelry, homes, clothes, etc.
b. Significant personal debt and credit problems-creditors appearing at the workplace.
c. Behavioral changes: may be an indication of drugs, alcohol, gambling, or fear of losing a job.
d. High employee turnover, especially in areas more vulnerable to fraud.
e. Refusal to take vacation or sick leave.
f. Lack of segregation of duties in the vulnerable area.
g. Taxpayer complaints that they are receiving non-payment notices.
h. Discrepancies between bank deposits and posting.
i. Abnormal number of expense items, supplies or reimbursement to an employee.
j. Bank Accounts that are not reconciled on a timely basis.
k. Falsifying time sheets: inconsistent overtime charged, overtime charged during a slack period or overtime charged for an employee not normally having overtime wages.
l. Purchasing: increased complaints on products, charges without shipping documents, high volume of purchases from new vendors, purchases that bypass normal procedures, vendors without physical addresses or addresses that match employee addresses.
m. Refusal to inventory items for sale or inconsistent/sloppy inventory.
n. Rewriting records under the guise of neatness in presentation.
o. Alteration and/or destruction of original County documents and records not in accordance with procedures indicated above.
p. Frequent detection of potentially malicious software on user's workstation which could

indicate an attempt to compromise or allow compromise of network security to mask actions or to allow actions of a 3rd party to affect network security.

2. Management Red Flags may include, but are not limited to:

a. Reluctance to provide information to auditors and/or frequent changes in external auditors.
b. Managers engage in frequent disputes with auditors.
c. Management decisions are dominated by an individual or small group.
d. Managers display significant disrespect for regulatory bodies.
e. Weak internal control environment.
f. Accounting personnel lax in their duties.
g. Decentralization without adequate monitoring.
h. Excessive number of checking accounts and/or frequent changes in banking accounts.
i. County assets sold under market value.
j. Excessive number of year end transactions.
k. High employee turnover.
l. Photocopies or missing documents.
m. Service contracts with no resulting product.
n. Request for significant funding in an unused budget line.

3. Public Red Flags may include, but are not limited to:

a. There is a recent and significant increase in the volume of activity pertaining to an existing account.
b. Documents are provided for identification that appear to have been altered or forged.
c. The photograph or physical description on an identification presented is not consistent with the appearance of the person presenting the identification.
d. Other information in documents provided for identification is not consistent with the individual presenting the information.
e. The document presented appears to have been altered or forged or gives the appearance of having been destroyed and recreated.
f. A phone number or address provided is invalid, a mail drop or a prison address.
g. The personal information presented is not consistent with the personal identification provided.
h. Mail sent to the customer is returned as undeliverable although transactions continue to occur with regard to the individual.

4. Third Party Red Flags:

a. A financial institution identifies a suspicious transaction involving County funds.
b. A consumer reporting agency provides a credit freeze in response to a request for a consumer report.

## VI. Detection of Red Flags:

1. The County shall require any two of the following three (3) primary forms of identification to verify

the identity of the person in question requesting sensitive information:

a. A valid NYS Driver's License or Identification Card;
b. A valid US Passport;
c. A valid US Green Card; and one of the following:
   - An original bill from an electric, gas, cable or other utility;
   - An original or certified copy of a birth certificate;
   - An original or certified copy marriage and/or divorce decree with a notarized signature; and/or
   - Court order, subpoena or other judicial documentation demanding access and/or documents.

2. The County shall utilize the following steps to detect employee and management red flags:

a. Create and regularly update internal controls for all departments;
b. Conduct periodic petty cash audits;
c. Regularly inventory files containing sensitive information; and
d. Monitor the County budget and report the County's financial position regularly to the County Board of Supervisors.

## VII. County's Responses to Red Flags:

In the event that a Red Flag is identified, the employee identifying the Red Flag shall immediately notify their supervisor. The employee's supervisor acting on behalf of the County shall determine whether or not a response is warranted upon a review of the information provided. If the supervisor determines a response is warranted, the supervisor shall notify the County Administrator, Director of Information Technology, Director of Human Resources and County Attorney, immediately after notifying law enforcement so that law enforcement may take all appropriate action.

## VIII. Policy Violations:

The County Attorney along with the Director of Information Technology shall be responsible for developing, implementing and updating this policy. The County Attorney along with the Director of Information Technology shall also be responsible for reviewing and updating this policy annually and presenting any changes to the Board of Supervisors for approval as is necessary and appropriate.

Mandatory annual training concerning Red Flags shall be implemented and provided by the Director of Information Technology for all employees granted access to the County's computer network in cooperation with Department Heads. Failure of an employee to complete mandatory training on an annual basis may result in limited access or a denial of access to the County computer network pending completion of the required annual training within a reasonable time period.

## IX. County Policy Administration and Updating:

Any violation of this policy by an employee of the County shall be investigated by the employee's appointing authority with assistance from the County Attorney's Office, Human Resources Department, and

the Department of Information Technology. All appropriate disciplinary and/or legal action shall be taken by the employee's appointing authority in accordance with collective bargaining agreements, Civil Service Law, section 75 regulations, and/or "employee at will" discipline/termination proceedings.

# Attachment A

## COUNTY OF WARREN COMPUTER NETWORK CONFIDENTIALITY AGREEMENT

This agreement is made between _____ (hereafter, "employee") and the County of Warren and the employee acknowledges that they received a copy of the Warren County Policy and Program for Red Flags Identity Theft Prevention and read the same and now accept and agree to comply with each and every term stated below in consideration of the employee's continued access and use of the County computer network, to include email and stored data, as follows:

1. The employee acknowledges that, in course of employment for the County of Warren, the employee has, and may in the future, come into the possession of certain confidential information including but not limited to names, addresses, dates of birth, social security numbers, protected health information, passwords, correspondence, and files of a sensitive or proprietary nature and that the employee accepts and agrees that they will at no time during or after their term of County employment, disclose or divulge to another any such confidential information, nor shall the employee use or disseminate for their own benefit or the benefit of another any such confidential information.
2. The employee promises and agrees that upon termination of employment, the employee will return to the County of Warren all physical documents and data relating to the County of Warren' business activities which contain any confidential information and are not available to the public upon the County's website and shall not retain any copies of such material or data to include, but not limited to: correspondence, reports, manuals, computer programs, and all other material and all copies of such material obtained by the employee during employment.
3. Violation of this agreement by an employee of the County shall be investigated by the employee's department, Director of Information Technology, and County Attorney's Office and all appropriate disciplinary action may be taken by the employee's appointing authority in accordance with collective bargaining agreements, Civil Service Law, section 75 regulations, and/or "employees at will" disciplinary/termination proceedings.
4. Violations of this agreement by an employee of the County may also result in a criminal action, a civil action for equitable relief and monetary damages, and/or administrative action against the employee.
5. Employees will not use County account passwords of similar passwords for any personal accounts unrelated to County operations. Employees when asked to choose passwords will not use a passwords or similar password to any passwords they use on personal non-County related accounts.

Employee Signature: _____ Dated:_____

Employee Name (Printed: _____

*A copy of this agreement shall be retained and filed in the employee's permanent personnel file.*