Warren County Board of Supervisors

RESOLUTION NO. 233 OF 2026

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

ADOPTING THE WARREN COUNTY POLICY AND PROGRAM FOR RED FLAGS IDENTITY THEFT PREVENTION

WHEREAS, the Risk and Safety Committee recommended and the Personnel Committee agreed to approve the Warren County Policy and Program for Red Flags Identity Theft Prevention and recommended that the same be advanced to the Board of Supervisors for consideration and adoption, now, therefore, be it

RESOLVED, that the Warren County Policy and Program 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, and be it further

RESOLVED, that any and all prior Warren County Program for Red Flags Identity Theft Prevention Policies, Resolutions or parts thereof inconsistent with the annexed Warren County Policy and Program for Red Flags Identity Theft Policy are hereby repealed effective June 18, 2026, and be it further

RESOLVED, that the Warren County Policy and Program for Red Flags Identify Theft Prevention will automatically be incorporated into the Warren County Risk and Safety Manual which was adopted by the Warren County Board of Supervisors on January 16, 2026.

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

I. Policy Statement:

The County of Warren 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 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 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, 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 requires 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.

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:

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.

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

Freedom of Information Law (FOIL): Freedom of Information Law per the NYS Public Officers Law Article 6 §84-90.

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

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.

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

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 required to use common sense judgment in securing sensitive information. Any County document marked "Confidential" or "Privileged and Confidential" by an authorized County employee is not for public distribution, except as required by the County's legal process and/or the Freedom of Information Law (FOIL).

Every County officer and employee responsible for the handling of sensitive information shall be required to sign a ***"County of Warren Sensitive Information Confidentiality Agreement"*** (Attachment A) in addition to any federal and state regulatory and statutory requirements. Department Heads and/or their designee shall determine the employees required to execute the ***County of Warren Sensitive Information Confidentiality Agreement*** in accordance with this policy.

Upon the adoption of revisions to this policy by the Board of Supervisors, every County employee, officer and agent shall receive a copy of the revised policy and shall acknowledge receipt of the policy via the County's online portal or by executing the acknowledgment in writing and providing the written acknowledgment to the Department of Human Resources.

A. 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 disposed of in accordance with department disposal protocols. 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. 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.

h. A request in writing by an employee for viewing of his/her permanent personnel file may be honored with verification of identity as prescribed in Section VI of this policy **and in accordance with the "Freedom of Information/Personnel Files" policy found in the County's Personnel Manual.** A record of the viewing and/or release of such documents shall be kept in accordance with the NYS Retention Schedules.

i. Requests for documents containing sensitive information shall only be honored with verification of identity as prescribed in Section VI 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 emails sent and received within the County email system are the property of the County, as more fully set forth in the County **Computer Use Policy**. Emails sent through the County e-mail system may be monitored under the provisions of the U.S. Electronics Communication Privacy Act (ECPA) and Computer Use Policy.

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

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. <u>Employee Red Flags may include, but are not limited to:</u>

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. Vendor 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 one (1) 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; or
b. A valid US Passport; or
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 shall notify their Department Head and/or their designee who acting on behalf of the County shall determine whether or not a response is warranted upon a review of the information provided. If the Department Head and/or their designee determines a response is warranted, the Department Head and/or their designee shall notify the County Administrator, Director of Human Resources (if the breach involves an employee's information), and County Attorney, immediately after notifying law enforcement so that law enforcement may take action as deemed appropriate.

VIII. Policy Violations:

Any violation of this policy by an employee of the County shall be investigated by the County Attorney's Office and 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.

IX. County Policy Administration and Updating:

The County Risk and Safety Committee shall be responsible for developing, implementing and updating this policy and shall provide updates to the Personnel Committee and Board of Supervisors for consideration as may be necessary.

Mandatory annual training concerning Red Flags shall be implemented and provided by the Risk and Safety Committee for all employees identified as having access to sensitive information.

Attachment A

COUNTY OF WARREN SENSITIVE INFORMATION 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 access to sensitive information within their County workplace, 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 sensitive 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 sensitive information, nor shall the employee use or disseminate for their own benefit or the benefit of another any such sensitive 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 sensitive 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 Head, and County Attorney's Office and appropriate disciplinary action may be taken 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.

Employee Signature: _____ Dated:_____

Employee Name (Printed: _____

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

ADOPTED BY A UNANIMOUS VOTE OF THOSE PRESENT