PERSONNEL COMMITTEE
AGENDA
MAY 29, 2026

Committee Members: ***Runyon, Crocitto, Driscoll, Etu, Maday, Turner, Conover- Chair of the Board shall serve as an Ex-Officio member when needed in accordance with Section C(4) of the Rules of the Board***

I. Committee meeting called to order by Chair.

II. Motion to approve minutes of prior Committee meetings.

III. Privilege of the Floor/Public Comment

IV. Action Agenda

1) **Notice of Intent to Fill Tracking Report** - provided for informational purposes

2) **Referrals from the Warren County Risk and Safety Committee*:***

A) Request to adopt the Warren County Lithium-Ion Battery and Cell Policy as recommended by the Warren County Risk and Safety Committee on May 6, 2026, after identifying the absence of a Board of Supervisors approved policy which establishes protocols to ensure compliance with New York State laws.

B) Request to adopt the updated Warren County Policy Program for Red Flags Identity Theft Prevention as recommended by the Warren County Risk and Safety Committee on May 6, 2026, after identifying the absence of a Board of Supervisors approved policy which establishes protocols to ensure compliance with New York State laws.

V. Pending Items: None.

VI. Privilege of the Floor/Public Comment

VII. Motion to adjourn

ITEM 1

2026 - NOTICE OF INTENT TO FILL TRACKING

Approval Date	Department	Position	Incumbent	Reason for Vacancy *	Incumbent Salary	Salary Approved	Date Filled	Hire	Salary Hired	Approved vs. Hired	Incumbent vs. Hired
11/12/2025	Social Services	Assistant SS Attorney # 3 (2831)	Leahy	PR	$ 95,391.00	$ 95,391.00	1/5/2026	Russell	$90,889.00	$ (4,502.00)	$ (4,502.00)
12/1/2025	Social Services	Intake Clerk # 8 (2660)	Dezalia	PR	$ 41,409.00	$ 40,729.00	2/17/2026	Paliulis	$42,053.00	$ 1,324.00	$ 644.00
12/12/2025	Social Services	Caseworker # 44C (2851)	N/A	N	N/A	$ 59,131.00	3/9/2026	Madia	$59,131.00	$ -	$ -
12/12/2025	Social Services	Caseworker # 45C (2852)	N/A	N	N/A	$ 59,131.00	3/9/2026	Williams	$59,131.00	$ -	$ -
12/12/2025	Social Services	Sr Caseworker # 11C (2853)	N/A	N	N/A	$ 62,900.00	1/5/2026	Nassivera	$65,600.00	$ 2,700.00	$ -
12/22/2025	Social Services	Caseworker # 37 (2558)	Nassivera	PR	$ 61,696.00	$ 59,131.00	1/5/2026	York	$59,131.00	$ -	$ (2,565.00)
12/29/2025	Countryside	Laundry Worker # 1 (1871)	N/A	N	N/A	$ 40,452.00	1/2/2026	LaMontain	$40,452.00	$ -	$ -
12/29/2025	Countryside	Institutional Aide # 19 (2746)	Lamontain	O	$ 42,755.00	$ 42,053.00	1/5/2026	Ladouceur	$42,053.00	$ -	$ (702.00)
1/7/2026	County Clerk	MV License Registration Clerk # 10 (1117)	Walker	RS	$ 48,924.00	$ 48,924.00	4/6/2026	Kocsis	$50,369.00	$ 1,445.00	$ 1,445.00
1/7/2026	DPW	MEO (M) # 33 (2846) W/CDL	N/A	N	N/A	$ 59,816.00	1/12/2026	Aldrich	$59,816.00	$ -	$ -
1/7/2026	Office for the Aging	Mealsite Manager # 7 (1943)	Millington	RT	$ 37,112.00	$ 29,813.00	1/14/2026	Gardner	$29,813.00	$ -	$ (7,299.00)
1/13/2026	Workforce Development	Fiscal Coordinator (2832)	Wilson	RS	$ 57,614.00	$ 57,614.00	1/13/2026	Wood	$57,614.00	$ -	$ -
1/13/2026	Public Defender	15th Assisant Public Defender (2840) Per Diem	N/A	N	N/A	64.37/hr	1/16/2026	Muller	64.37/hr	$ -	$ -
1/16/2026	Social Services	Support Investigator # 5 (1739)	Havill	RS	$ 48,924.00	$ 48,924.00	3/23/2026	Howe	$49,627.00	$ 703.00	$ 703.00
1/16/2026	Social Services	Social Welfare Examiner # 15 (1718)	Gurlick	RS	$ 48,924.00	$ 48,924.00	3/9/2026	Perez-Torres	$50,369.00	$ 1,445.00	$ 1,445.00
1/21/2026	DPW	MEO (L) # 27 (2256)	McKeown	RS	$ 56,653.00	$ 56,653.00	2/9/2026	Babbie	$56,653.00	$ -	$ -
1/28/2026	Social Services	Caseworker # 42 (2743)	Leonard	RS	$ 60,756.00	$ 59,131.00	4/6/2026	Kostek	$60,756.00	$ 1,625.00	$ -
1/28/2026	Social Services	Intake Clerk # 13 (2854)	N/A	N	N/A	$ 42,053.00	2/9/2026	Alber	$42,053.00	$ -	$ -
1/29/2026	County Attorney	2nd Asst County Attorney (2442)	Dickey	PR	$ 111,875.00	$ 115,510.00	vacant				
1/30/2026	Public Defender	14th Asst Public Defender (2822)	N/A	O	N/A	$ 91,177.00	1/29/2026	Rienzo	$91,177.00	$ -	$ -
1/30/2026	Public Defender	10th Asst Public Defender (2755)	N/A	O	N/A	$ 91,177.00	1/29/2026	Kurd	$91,177.00	$ -	$ -
2/2/2026	Planning	Principal Planner # 2 (2811)	Nelson	O	$ 84,093.00	$ 84,093.00	2/2/2026	Nelson	$84,093.00	$ -	$ -
2/9/2026	DPW	MEO (M) # 4 (1254)	Mitchell	PR	$ 58,130.00	$ 59,816.00	2/9/2026	Logue	$60,520.00	$ 704.00	$ 2,390.00
2/9/2026	DPW	MEO (M) # 14 (1261)	Parker	PR	$ 59,816.00	$ 59,816.00	2/9/2026	Brownell	$60,520.00	$ 704.00	$ 704.00
2/12/2026	Social Services	Caseworker # 23 (1672)	Mackey	RS	$ 59,131.00	$ 59,131.00	4/6/2026	Hayes	$59,131.00	$ -	$ -
2/12/2026	DPW	MEO (L) # 26 (1225)	Brownell	PR	$ 57,357.00	$ 50,413.00	2/23/2026	Weis	$50,413.00	$ -	$ (6,944.00)
2/13/2026	DPW	MEO (L) # 17 (1250)	Hammond	RS	$ 56,653.00	$ 56,653.00	2/17/2026	Miller	$56,653.00	$ -	$ -
2/13/2026	DPW	MEO (L) # 33 (2563)	Logue	PR	$ 57,357.00	$ 56,653.00	2/23/2026	Murphy	$56,653.00	$ -	$ (704.00)
2/19/2026	Social Services	SWE # 19 (1721)	Pratt	RS	$ 50,369.00	$ 48,924.00	3/16/2026	Finkle	$50,369.00	$ 1,445.00	$ -
2/20/2026	Workforce Development	E&T Counselor II # 1 (2696)	Mender	RT	$ 61,503.00	$ 53,576.00	2/23/2026	Rosenfield	$53,576.00	$ -	$ (7,927.00)
2/20/2026	Public Defender	Coordinating Asst PD (2588)	Nicols	RS	$ 114,986.00	$ 114,986.00	2/24/2026	Whitney	$114,986.00	$ -	$ -
2/24/2026	Treasurer	Principal Account Clerk #3 (1094)	N/A	N	N/A	$ 52,138.00	3/16/2026	Thompson	$52,138.00	$ -	$ -
2/24/2026	Office for the Aging	Meal Site Manager # 9 (1949)	Simola	RS	$ 30,339.00	$ 29,813.00	3/2/2026	Ostrander	$29,813.00	$ -	$ (526.00)
2/24/2026	Public Defender	5th Assistant Public Defender (1078)	Whitney	PR	$ 105,949.00	$ 105,949.00	2/24/2026	Lowe	$105,949.00	$ -	$ -
2/26/2026	Social Services	Intake Clerk (1754)	Perez-Torres	PR	$ 43,380.00	$ 42,053.00	4/6/2026	Alber	$42,053.00	$ -	$ (1,327.00)
3/3/2026	Social Services	Medicaid Clerk # 2 (2094)	Finkle	PR	$ 44,848.00	$ 43,495.00	vacant				
3/3/2026	DPW	Construction Specialist II (2855)	N/A	N	N/A	$ 96,589.00	3/9/2026	Johnson	$96,589.00	$ -	$ -
3/11/2026	Social Services	Intake Clerk # 11 (2791)	Howe	PR	$ 42,755.00	$ 42,053.00	4/13/2026	Sears	$42,053.00	$ -	$ (702.00)
3/11/2026	DPW	MEO (L) # 3 (1249)	Frasier	RS	$ 57,357.00	$ 50,413.00	3/16/2026	Carpenter	$50,413.00	$ -	$ (6,944.00)
3/12/2026	Social Services	Intake Clerk # 7 (2406)	Kocsis	RS	$ 43,380.00	$ 42,053.00	4/13/2026	Patrick	$42,053.00	$ -	$ (1,327.00)
3/19/2026	Veterans' Services	Office Specialist (2425)	Aprile	O	$ 47,238.00	$ 47,238.00	3/23/2026	Vredenburgh	$47,238.00	$ -	$ -
3/19/2026	DPW	Director of Parks, Recreation (1185)	Moore	RT	$ 86,669.00	$ 86,669.00	3/23/2026	Inglee	$86,669.00	$ -	$ -
3/19/2026	Treasurer	Senior Account Clerk #4 (1086)	Thompson	PR	$ 47,238.00	$ 47,238.00	4/6/2026	Curry	$47,238.00	$ -	$ -
3/30/2026	Public Defender	Legal Clerk II (2841)	N/A	N	N/A	$ 48,924.00	4/6/2026	Davis	$48,924.00	$ -	$ -
4/8/2026	Human Resources	Civil Service Assistant-PT (2568)	Green	O	$ 40,436.92	$ 40,436.92	4/20/2026	Wilken	$40,436.92	$ -	$ -
4/8/2026	Human Resources	Civil Service Assistant-Temp (2594)	Green	O	25.92/hr	25.92/hr	4/20/2026	Green	25.92/hr	$ -	$ -
4/9/2026	Social Services	Caseworker # 36 (2557)	Kostek	O	$ 60,756.00	$ 59,131.00	4/20/2026	Dunning	$59,131.00	$ -	$ (1,625.00)
4/14/2026	Public Defender	Case Manager # 2 (2842)	N/A	N	N/A	$ 56,173.00	4/20/2026	Wilcox	$56,173.00	$ -	$ -
4/14/2026	Public Defender	7th Assistant PD (2419)	Wodicka	RS	$ 102,546.00	$ 102,546.00	4/20/2026	O'Neil	$102,546.00	$ -	$ -
4/16/2026	Veterans' Services	Van Driver # 5 (Per-Diem) (2518)	Cooke	RS	14.2958/ hr	19.1106/ hr	5/4/2026	Funnye	19.1106/hr	$ -	4.8148/hr
4/22/2026	Planning	Senior Planner (2414)	N/A	O	N/A	$ 62,900.00	5/7/2026	Smith	$63,604.00	$ 704.00	$ -
4/22/2026	Planning	Junior Planner (2483)	Smith	PR	$ 54,280.00	$ 53,576.00	vacant				
5/1/2026	Health Services	Deputy Director Health Services (2787)	Belden	PR	$ 117,442.00	$ 98,023.00	5/4/2026	Shah	$98,023.00	$ -	$ (19,419.00)
5/7/2026	DPW	Hatchery Aide (1197)	Whalen	PR	$ 47,146.00	$ 45,079.00	5/18/2026	Freebern	$45,079.00	$ -	$ (2,067.00)
5/8/2026	Public Defender	9th Assistant Public Defender (2608)	Lowe	PR	$ 94,906.00	$ 94,906.00	vacant				
									Total:	$8,297.00	$ (57,249.00)

* (RT= Retired, RS= resigned, PR= promotion, O= Other, N- New)

RESOLUTION REQUEST FORM NO. 20

MISCELLANEOUS

Please List All Other Requests Not Covered by Previous Resolution Request Forms Here. Please attach any backup information available and be as detailed as possible.

DEPARTMENT NAME: **County Attorney**

DATE: **5/29/26**

(a) Purpose of Request: **Adopting the Warren County Lithium-Ion Battery and Cell Policy**

(b) Details: **The Risk & Safety Committee approved the proposed Policy for Lithium-Ion Battery and Cells on May 6, 2026 after identifying the absence of a Board of Supervisors approved policy which establishes protocols to ensure compliance with New York State laws. The proposed policy will provide uniform and consistent standards for Lithium-Ion Battery and Cells.**

(c) Previous Resolution Number:

(d) Where are the Funds (if required)? List Budget Code, Object Code, Full Title* and Amount:

Sample: A.8021 470 Planning & Community Development – Contract

* as listed in budget and LOGOS

County Lithium-ion Battery and Cell Policy To Personnel Committee

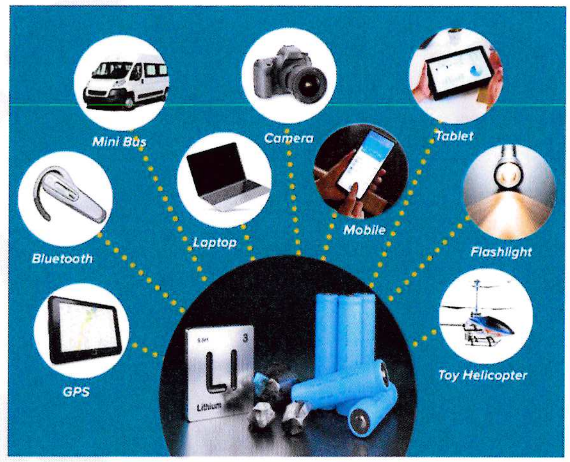
Title: Lithium-ion Battery and Cell Safety Program

I. Purpose

Lithium-ion batteries and cells are regulated under the OSHA Hazard Communication Standard 29 CFR 1910.1200 and the General Duty Clause requiring employers – the County to manage the risks of fire, explosion, and chemical exposures present during the use and storage of lithium-ion batteries. The County shall adopt the following guideline to provide employee users of lithium-ion (Lithium-ion) and lithium polymer (LiPo) cells and battery packs with enough information to safety handle them under normal and emergency conditions. The County urges caution be taken in Lithium-ion battery storage, use, management, and disposal due to the potential for fire and injury if these batteries are misused, damaged and/or stored incorrectly.

II. Lithium-ion Battery Basics

Lithium-ion batteries supply power to many kinds of devices including smart phones, laptops, e-scooters and e-bikes, e-cigarettes, smoke alarms, toys, and even cars. If not used correctly, or if damaged, these batteries have the potential of catching on fire or exploding.



Lithium-ion batteries are easily rechargeable and can store large amounts of energy in a small space. If not treated properly, lithium-ion batteries can overheat, creating thermal runaway, which causes large, violent fires.

Damaged, defective, or uncertified lithium-ion batteries have a greater risk of causing thermal runaway fires or explosions.

If the cells and batteries are correctly handled, the risk of fire developing from a lithium-ion battery from a reputable manufacturer is very low. Most incidents involving lithium-ion batteries find a root cause in the mishandling or unintended abuse of such batteries. Possible causes of lithium-ion battery fires include over charging or discharging; unbalanced cells; excessive current discharge; short circuits; physical damage; excessive hot storage; the storage of multiple lithium-ion cells in a pack; and poor electrical connections when in use.

The following generic criteria should be used when handling and using lithium-ion batteries and cells:

- Always purchase batteries and chargers from a reputable manufacturer or supplier. Cheap or counterfeit batteries and chargers may not undergo the same quality control processes and have a higher likelihood of failing.
- Be sure to read all documentation supplied with your battery.
- Use the battery designed for your device.
- Use the manufacturer recommended charger for the device you are charging.
- Stop using the battery if it's damaged.
- Never burn, overheat, disassemble, short-circuit, solder, puncture, crush or otherwise mutilate battery packs or cells for use of a device.
- Immediately disconnect the batteries if, during operation or charging, they emit an unusual smell, develop heat, change shape, or behave abnormally.
- Do not leave batteries connected to chargers after charging is complete or over-charge them.

Industry standards recommend the following protocols for lithium-ion batteries and cells:

County Lithium-ion Battery and Cell Policy To Personnel Committee

- Store batteries in a dry and well-ventilated place at room temperature whenever possible. Don't leave them in a hot car, in direct sunlight, or in freezing temperatures. Storage areas should be maintained free from any materials which can catch fire such as wood tables, carpet, or gasoline containers. The ideal surface for storing lithium-ion batteries is concrete, metal, or ceramic or any non-flammable material.
- Batteries can be stored in a metal cabinet such as a chemical-storage cabinet, make sure that batteries are not touching each other.
- Always inspect batteries for any signs of damage before use. Never use and promptly dispose of damaged or puffy batteries. Contact Building and Grounds for proper disposal.
- Do not mix different types of batteries or mix new and old ones together (e.g. in a power pack).
- Do not open the battery system or modules.
- Store lithium batteries with no more than 30-50% of their charge for long-term storage.

III. Responsibilities

Department Heads and/or their designees who purchase lithium-ion batteries for County use shall be responsible for:

- Implementation of all applicable provisions of this policy and its protocols;
- Ensure employees in possession of County provided lithium-ion batteries are trained on this procedure and its proper response actions;
- Conduct an analysis of what lithium battery technology is maintained within their department and where; and
- Ensure purchasing of lithium-ion batteries and chargers comply with this policy.

Employees who use County supplied lithium-ion batteries shall be responsible for following the policy as outlined.

IV. Shipment and/or Disposal of County Owned Lithium-ion Batteries and Cells

Only trained and authorized personnel are allowed to prepare, package, and ship lithium-ion batteries and cells. If you are planning to ship lithium-ion batteries, with or without equipment, please follow the manufacturer's directions for shipment and/or disposal.

It is unlawful to throw out lithium-ion batteries in the County's regular waste. By law, lithium-ion batteries and cells must be recycled. Damaged lithium-ion batteries require special disposal methods. Please contact the County Building and Grounds department for proper disposal.

V. Emergency Procedures Involving Lithium-ion Batteries and Cells

A. Warning Signs of a Lithium-Ion Battery and Cells Fire:

- **If the device is hot**: It is normal for batteries to generate some heat when they are charging or in use. If your device's battery feels extremely hot to your touch, it is likely defective and at risk to start a fire.
- **If the device is swelling or bulging**
- **If the device is making a noise:** Device is making a hissing, cracking, or popping sound.
- **If the device has an odor**: Pay attention to any strong or unusual odors coming from the battery. Lithium-ion batteries emit toxic fumes when they fail.

If you notice any of the warning signed noted above from a County purchased lithium-ion battery or cell:

- Stop using the device and turn it off immediately.
- Unplug it from the power source.
- Leave the area.

County Lithium-ion Battery and Cell Policy To Personnel Committee

B. Responding to Smoking or Overheating Device:

- **Do not touch or move the device.** Thermal runaway generates a dangerous amount of heat and can release toxic fumes that could be spread through the building.
- **Immediately evacuate** the area and activate the nearest fire alarm pull station or initiate evacuation verbally.
- **Do not try to put the fire out yourself**. Lithium-ion battery fires spread quickly, aggressively, and can become explosive, or reignite. Water may not prevent a battery from burning and fire extinguishers do not work on lithium-ion battery fires.
- Follow the instructions of your emergency evacuation plan.

RESOLUTION REQUEST FORM NO. 20

MISCELLANEOUS

Please List All Other Requests Not Covered by Previous Resolution Request Forms Here. Please attach any backup information available and be as detailed as possible.

DEPARTMENT NAME: COUNTY ATTORNEY

DATE: 5/29/2026

(a) Purpose of Request: **To approve and adopt the updated "Warren County Policy Program for Red Flags Identity Theft Prevention"**

(b) Details: **See attached redlines that were recommended by the Risk & Safety Committee**

(c) Previous Resolution Number: **485 of 2024**

(d) Where are the Funds (if required)? List Budget Code, Object Code, Full Title* and Amount: **None.**

Sample: A.8021 470 Planning & Community Development – Contract

* as listed in budget and LOGOS

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

I. Policy Statement:

The ~~Warren~~ County of Warren Policy for Identity 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~~ 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.

~~The policy will assist the County:~~

1. ~~Identify 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:

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.

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

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~~ required to use common sense judgment in securing ~~personal identifiable~~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 an ***"~~Employee~~ County of Warren Sensitive Information Confidentiality Agreement"*** ~~for the County of Warren~~ ***(Attachment A)*** in ~~additionto~~addition to ~~addition to~~ any federal and state regulatory and ~~statutoryrequirements~~statutory requirements. ~~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.~~ 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.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold, Not Italic

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 acknowledgement in writing and providing the written acknowledgement to the Department of Human Resources.

~~. 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.)~~

~~0. Planning and Economic Development: Loan, Grant and Assistance Applications;~~
~~0. Human Resources and Self-Insurance Departments: Payroll, Retiree, Employment, and Workers Compensation Records;~~
~~0. County Clerk's Office, including Birth Records; Death Records; Marriage Licenses;~~
~~0. Sheriff's Office;~~
~~0. Department of Social Services;~~
~~0. Department of Health Services;~~
~~0. County Attorney's Office;~~
~~0. County Public Defender's Office;~~
~~0. Information Technology Department/Computer Network Security.~~

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.

ITEM 2B

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

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~~disposed of in accordance with department disposal protocols. Documents considered municipal records, ~~however~~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 New York State Department of Health.

~~g. Sheriff Department documents are secured per the Sheriff Department Policy and NYSPIN regulations.~~

~~h.~~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.

~~i.~~h. A request in writing by an employee for viewing of his/her permanent personnel file ~~shall only~~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 ~~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 NYS Retention Schedules.

Commented [CM1]: I have this circled in my notes?

~~j.~~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 NYS Retention Schedules.

2. **Electronic Document Management:**

a. The County's e-mail system is a County-owned system. All ~~e-mails~~emails sent and received within the County e-mail system are the property of the County, as more fully set forth ~~by~~ in the ~~Warren~~ County **Computer ~~Usage~~ Use Policy**~~, approved by Resolution 144 of 2023~~. ~~E-mails~~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 ~~Usage~~ Use Policy.

~~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:~~

- ~~Be classified by Civil Service as full-time, part-time, seasonal, or an intern.~~
- ~~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.~~
- ~~A signed "Acknowledgement 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.~~
- ~~A signed "Warren County Confidentiality Agreement"~~

~~b. 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.~~

~~b. All employees must comply with the "Computer Use Policy," found in Resolution 410 of 2024, and any future updates to the Computer Usage Policy.~~

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

Formatted: Justified, Right: 0.08", Don't allow hanging punctuation, Tab stops: 0.5", Left

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

b. ~~"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."~~

~~d.~~c. 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.

~~e. 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.~~

~~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.~~

~~f. The County shall maintain a cyber block/black list and enforcement shall be on the network perimeter.~~

~~Wireless networks shall never be used when conducting financial transactions.~~

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

~~i. Administrative passwords shall be periodically changed, including routers, firewalls, other network equipment and software. Factory default passwords shall not to be used on security equipment and systems.~~

~~i. 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.~~

~~i. 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.~~

~~i. 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.~~

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

~~i. 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.

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

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~~ 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.

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:

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

1. The County shall require any ~~two~~ 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~~supervisor~~ determines a response is warranted, the Department Head and/or their designee ~~supervisor~~ shall notify the County Administrator, ~~Director of Information Technology~~, 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 ~~all appropriate~~ 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 ~~with the assistance of the Department of Information Technology~~ 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, ~~s~~Section 75 regulations, and/or "employee at will" discipline/termination proceedings.

IX. County Policy Administration and Updating:

~~The County Attorney along with the Director of Information Technology~~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. ~~The County Attorney along with the Director of Information Technology shall also 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~~Risk and Safety Committee 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~~identified as having access to sensitive information.

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

Attachment A

COUNTY OF WARREN ~~COMPUTER NETWORK~~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 ~~continued access and use of the County computer network, to include email and stored data~~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 ~~confidential~~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 ~~confidential~~sensitive information, nor shall the employee use or disseminate for their own benefit or the benefit of another any such ~~confidential~~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 ~~confidential~~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, correspondence, 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~~Department Head, ~~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~~ 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 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.~~

Formatted: Right: 0.08"

Employee Signature: ______________________________ Dated: ______________

Employee Name (Printed): ______________________________

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