

LEGISLATIVE, RULES & GOVERNMENT OPERATIONS
INFORMATION TECHNOLOGY AGENDA
NOVEMBER 29, 2023

Committee Members:

STROUGH, Conover, Frasier, Geraci, Thomas, Driscoll and Wild

- I. Committee meeting called to order by Chair
- II. Approval of minutes of prior Committee Meeting
- III. Privilege of the floor and public comment
- IV. Action Agenda/New Business Items:
 1. Request: Adopt updated Computer Breach Notification policy.
Rationale: Needs updating.
 2. Request:
Rationale:
- V. Discussion Items:
 1. Shared Services
- VI. Referrals/Pending Items:
- VII. Privilege of the floor and public comment
- VIII. Motion to adjourn

Attachments:

1. Miscellaneous 20
2. Computer Breach Notification Policy

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: Information Technology

DATE: November 2023

- (a) Purpose of Request: **Update Computer Breach Notification Policy**
- (b) Details: **Attached**
- (c) Previous Resolution Number: **n/a**
- (d) Where are the Funds (if required)? List Budget Code, Object Code, Full Title* and Amount: **none needed**

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

*** as listed in budget and LOGOS**

**POLICY IMPLEMENTING STATE TECHNOLOGY LAW §208
REQUIREMENTS FOR NOTIFICATION WHEN A PERSON
WITHOUT VALID AUTHORIZATION HAS ACQUIRED PRIVATE INFORMATION**

I. PURPOSE: The purpose of this Resolution is to adopt, in compliance with State Technology Law § 208, the Warren County Policy Implementing Requirements for Notification When a Person Without Valid Authorization Has Acquired Private Information. Any particulars not determined in this policy shall be construed within the provisions of the State Technology Law § 208.

II. TERMS AND MEANINGS: As used in this section, the following terms shall have the following meanings:

a) “Private information” shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired.

- 1) social security number;
- 2) driver’s license number or non-driver identification card number; or
- 3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual’s financial account;
- 4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual’s financial account without additional identifying information, security code, access code, or password; or
- 5) biometric information, meaning data generated by electronic measurements of an individual’s unique physical characteristics, such as

fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

- 6) a user name or email address in combination with a password or security question and answer that would permit access to an online account.

“Private Information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

b) “Breach of the security of the system” shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information used or owned by the County. Good faith acquisition of personal information by an employee or agent of the County for the purposes of the County is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, a Department head may consider the following factors, among others:

- 1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- 2) indications that the information has been downloaded or copied; or
- 3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

c) “Consumer reporting agency” shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be obtained from the state attorney general.

d) “Department Head” shall mean a Warren County Department Head.

III. NOTIFICATION: a) Any Department Head whose department owns and/or controls computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The Department Head shall consult with the technical support personnel/vendor to determine the scope of breach and restoration measures.

b) Any Department Head whose department operates computerized data that includes private information which such department does not own and/or control, shall notify the owner or licensee of the information of any breach of the security system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

c) Any Warren County employee who discovers or learns of any breach in the security of the system shall promptly report such breach to his or her department head.

d) The notification required by this policy may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this policy shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

e) The notice required by this policy shall be directly provided to the affected persons by one of the following methods:

- 1) written notice;
- 2) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the County who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition or establishing any business relationship or engaging in any transaction;
- 3) telephone notification provided that a log of each such notification is kept by the County who notifies affected persons; or
- 4) substitute notice, if a department head demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such Department Head does not have

sufficient contact information. Substitute notice shall consist of all of the following:

- i. Email notice when such department head has an email address for the subject persons;
- ii. Conspicuous posting of the notice on the County's website page;
- iii. Notification to major statewide media.

f) Regardless of the method by which notice is provided, such notice shall include contact information for the County department making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

g) In the event that any New York residents are to be notified, the Department Head shall notify the Warren County Attorney, the Consumer Protection Board, and the Warren County Information Technology Department as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

h) In the event that more than five thousand New York residents are to be notified at one time, the Department Head shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.