RESOLUTION NO. 274

ADOPTING AN INFORMATION SECURITY INCIDENT NOTIFICATION POLICY FOR ALBANY COUNTY

Introduced: 7/10/23
By Law Committee:

WHEREAS, The New York State Stop Hacks and Improve Electronic Data Security (SHIELD) Act strengthened data security laws by expanding the types of information for which companies must provide consumer notice in the event of a breach as well as requiring companies to establish safeguards to protect private information, and

WHEREAS, The Chief Information Officer has requested that this Honorable Body adopt an Information Security Incident Notification Policy in order to outline the steps Albany County employees should take in response to a suspected or confirmed information security incident and to comply with the SHIELD Act, now, therefore, be it

RESOLVED, By the Albany County Legislature that the Information Security Incident Notification Policy, annexed hereto, is hereby adopted, and, be it further

RESOLVED, That the Clerk of the County Legislature is directed to forward certified copies of the resolution the appropriate County Officials.

DANIEL P. MCCOY
COUNTY EXECUTIVE

M. DAVID REILLY
COMMISSIONER

PATRICK ALDERSON
DEPUTY COMMISSIONER

COUNTY OF ALBANY
DEPARTMENT OF MANAGEMENT AND BUDGET
DIVISION OF INFORMATION SERVICES
112 STATE STREET, ROOM 500
ALBANY, NEW YORK 12207
PHONE: (518) 447-7277 FAX: (518) 447-3000
www.albanycounty.com

ANDREW BELLINGER
CHIEF INFORMATION OFFICER

DAVID BERKUN
DEPUTY CHIEF
INFORMATION OFFICER

Category: TBD	Policy Title: Information Security Incident Notification Policy
Responsible Office: Division of Information Services (DIS)	Document Number: TBD Effective Date: TBD This policy item applies to: Albany County departments and its employees

Summary

Albany County is committed to securing and protecting the information within its possession. Albany County departments shall adhere to all applicable federal, state, and local laws and regulations related to incident reporting, data breach notification, and information security.

Policy Purpose

The purpose of the Albany County Information Security Incident Notification Policy is to provide a clear and concise process for required notifications in the event of a suspected or confirmed Information Security Incident.

According to the National Institute of Standards and Technology (NIST), an Information Security Incident is defined as:

An occurrence or event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Suspected or confirmed Information Security Incidents can be identified by anyone who has information related to the improper access or release of confidential and/or private information such as Protected Health Information (PHI) or Personal Identifiable Information (PII). This information can be identified through any avenue including personal knowledge of the incident or third-party notifications from outside entities.

Policy Details

Incident Reporting by County Departments:
All Albany County departments must follow established procedures for identifying and reporting security incidents promptly. In the event of an Information Security Incident within a department, employees are required to notify the Division of Information Services (DIS) immediately through the notifying procedures established below.

Reporting Security Incidents Involving Third-Party Vendors or Contractors:
Albany County departments must maintain a record of all third-party vendors and contractors with whom they have work relationships or agreements. If an Information Security Incident occurs involving a third-party vendor or contractor, the respective department must inform Division of Information Services as soon as they are made aware.

Security Incident Notification Procedures:
In the event that an employee or department within Albany County becomes aware of a suspected or confirmed Information Security Incident they must provide notification by one of the following ways:

- Contact the Albany County Helpdesk via telephone at 518-447-7200 option - 1
- Email the Albany County Cyber Incident Response Team at accirt@albanycountyny.gov

When contacting the Albany County Cyber Incident Response Team, please be prepared to provide the following information if it is available:

Information to include in the notification:
- Nature of the incident: Provide a clear description of the incident and its potential impact.
- Date and time: Specify when the incident occurred or was first noticed.
- Systems or data affected: Identify the specific systems, applications, or data that have been compromised or at risk.
- Initial findings or observations: Share any preliminary findings or observations related to the incident.
- Employees should include their contact information in the email for follow-up communication, if necessary.

Division of Information Services Procedures:
- Upon receiving a notification about an Information Security Incident, DIS will promptly evaluate the nature, severity, and potential impact of the incident. This evaluation will help determine the appropriate response actions, including incident containment, investigation, and notification requirements.
- The Division of Information Services, in conjunction with the Albany County Law Department, will be responsible for notifying the required New York State entities and Albany County users affected by the security incident.
- Notifications to external entities will be made in accordance with applicable laws, regulations, and contractual obligations.
- The Division of Information Services and the Albany County Law Department will collaborate to ensure that notifications are consistent, accurate, and appropriately authorized.

Policy Review and Maintenance:
This policy shall be reviewed regularly to ensure its effectiveness and alignment with changing technology landscapes, legal requirements, and industry standards. Updates or revisions to this policy should be communicated to all relevant departments and personnel.