City of Oneida – Data Breach Notification Policy

Adopted by Resolution No. ___ of the Common Council on [Date]

I. Purpose

The purpose of this policy is to ensure that the City of Oneida complies with the notification requirements of New York State Technology Law § 208 in the event of a breach of the City's information systems containing private information, and to establish procedures for prompt internal reporting, investigation, and external notification.

II. Scope

This policy applies to all departments, offices, boards, commissions, and employees of the City of Oneida, as well as contractors, consultants, volunteers, and vendors who access, store, or manage private information on behalf of the City.

III. Definitions

1. Private Information – As defined by New York State Technology Law § 208, private information means 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 is encrypted with an encryption key that has also been acquired:
- Social Security number.
- Driver's license number or non-driver identification card number.
- Account number, credit card number, or debit card number, in combination with any security code, access code, or password.
- Biometric information.

2. Breach of the Security of the System – Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of private information maintained by the City.

IV. Responsibilities

- City Manager – Serves as the Incident Response Coordinator for all breaches and oversees compliance with this policy.
- Total Solutions (Contracted IT Service Provider) – Leads the technical investigation, secures systems, and determines the scope of the breach. Total Solutions 24/7 Contact Number: Office: 315-724-9410- City Attorney – Provides legal guidance and ensures that notifications comply with state and federal law.
- Department Heads – Immediately report suspected breaches to Total Solutions and the City Manager.
- All Employees – Must report any suspected loss, theft, or unauthorized access to data to their supervisor or directly to Total Solutions.

V. Internal Reporting Procedure

1. Immediate Notification – Any employee who becomes aware of a possible breach must notify their Department Head immediately.
2. Escalation – Department Head must notify Total Solutions at 315-724-9410 and the City Manager within one (1) hour of learning of the breach.
3. Incident Log – Total Solutions will create an incident record documenting:

- Date and time breach was discovered.
- How the breach was discovered.
- Information believed to be compromised.

VI. Assessment & Containment

Total Solutions, in coordination with the City Manager, will promptly investigate to determine:
- Whether a breach occurred.
- The scope and nature of the compromised data.
- Whether law enforcement notification is required.

Immediate steps will be taken to contain the breach and prevent further unauthorized access.

VII. Notification Requirements

If the investigation confirms a breach of private information, the City will provide notice as follows:

1. Individuals Affected – Notify each individual whose private information was, or is reasonably believed to have been, acquired without valid authorization.
2. State Authorities – Notify:
   - New York State Office of the Attorney General.
   - New York State Office of Information Technology Services (ITS).
   - New York State Office of the State Comptroller (OSC).
3. Law Enforcement – If criminal activity is suspected, notify local law enforcement and/or the New York State Police Cyber Command.

VIII. Timing of Notice

Notification will be made in the most expedient time possible and without unreasonable delay, but no later than 30 days after the breach is discovered, unless law enforcement determines that notification would impede a criminal investigation.

IX. Content of Notice

Each notification will include, to the extent available:
- The date (or estimated date) of the breach.
- A description of the private information involved.
- A general description of the incident.
- Steps individuals should take to protect themselves.
- Contact information for the City for further assistance.

X. Methods of Notice

Notice may be provided by one or more of the following methods:
- Written notice via U.S. Mail.
- Electronic notice (if the individual has consented).
- Telephone notification.
- Substitute notice (posting on City website and in City Hall) if contact information is insufficient.

XI. Documentation

Total Solutions will maintain a permanent record of each breach, including:
- Incident reports.

- Copies of all notices sent.
- Steps taken to contain and remediate the breach.

XII. Prevention & Training

- Annual cybersecurity awareness training for all employees.
- Regular vulnerability scans and penetration tests.
- Review and update of this policy annually.

XIII. Policy Review

This policy shall be reviewed annually by the City Manager and Total Solutions, and updated as necessary to ensure compliance with applicable laws and best practices.

Appendix A – Sample Data Breach Notification Letter

[City of Oneida Letterhead]
City of Oneida
109 N. Main Street
Oneida, NY 13421
Tel: 315-363-4800
Email: info@oneidacityny.gov

[Date]

[Recipient Name]
[Address]
[City, State ZIP]

Subject: Notice of Data Security Incident

Dear [Recipient Name],

We are writing to inform you of a data security incident that may have involved your personal information. At the City of Oneida, we take the protection of your information very seriously, and we want to provide you with details about what happened, what information may have been affected, and what steps you can take to protect yourself...

Sincerely,
Kyle Lovell
City Manager
City of Oneida

Appendix B – Data Breach Incident Log Form

City of Oneida – Data Breach Documentation Record

Incident ID: _____
Date Reported: _____
Reported By: _____
Department: _____
Contact Info: _____

Section 1 – Initial Discovery
Date & Time Breach Discovered: _____
Person/Department Discovering Breach: _____
Description: _____

Section 2 – Breach Details
Type of Breach: _____
System(s) or Data Affected: _____
Estimated Number of Individuals Affected: _____
Type(s) of Private Information: _____

Section 3 – Containment Actions
Date & Time Containment Began: _____
Steps Taken: _____

Section 4 – Notifications
Law Enforcement: _____
State Agencies: _____
Individuals Notified: _____

Section 5 – Resolution & Remediation
Date Contained/Resolved: _____
Remediation Steps: _____

Section 6 – Post-Incident Review
Lessons Learned: _____
Policy/Procedure Changes Recommended: _____