

Village of Brownville

216 Brown Blvd.
Brownville, NY 13615
Phone:315-782-7650

RESOLUTION 4 OF 2026

ADOPTION OF POLICY CYBERSECURITY BREACH NOTIFICATION

WHEREAS, the Village Board of the Village of Brownville, New York is empowered to consider, draft, and adopt policies to address important aspects of good governance; and

WHEREAS, the Village Board has determined that a policy addressing Cybersecurity Breach Notification pursuant to NYS Technology Law §208 is appropriate; and

WHEREAS, the Village has prepared a policy to address Cybersecurity Breach Notification and a copy is attached as Exhibit "1".


NOW, THEREFORE, BE IT RESOLVED, by the Village Board of the Village of Brownville, New York as follows:

1. The foregoing recitations are incorporated herein and made a part hereof as if set forth hereafter.
2. The Village adopts the Cybersecurity Breach Notification Policy attached as Exhibit "1".
3. The Cybersecurity Breach Notification Policy shall be filed with the Village Clerk of the Village of Brownville and posted to the Village Website.
4. This resolution shall take effect immediately.

The foregoing Resolution was offered by Board Member, Mike Walrath, and seconded by Board Member, Amy Baker and upon roll call vote of the Board was duly adopted as follows:

	YES	NO
Patrick Connor, Mayor	X _____	_____
Steve Mott, Trustee	X _____	_____
Mike Walrath, Trustee	X _____	_____
Robert D. Goutremout, Trustee	X _____	_____
Amy Baker, Trustee	X _____	_____

Dated: March 10, 2026



Amber Klusacek, Village Clerk



PO BOX 118 • 216 BROWN BLVD • BROWNVILLE, NY 13615 • 315-782-7650
CLERK@VILLAGEOFBROWNVILLE.NY.GOV * WWW.VILLAGEOFBROWNVILLE.NY.GOV

Cybersecurity Breach Notification Policy Pursuant to New York State Technology Law Section 208

ADOPTED BY VILLAGE BOARD RESOLUTION 4 OF 2026

I. PURPOSE

The purpose of this policy is to establish a clear and consistent process for notifying individuals in the event of a cybersecurity breach that compromises their personal information. The Village of Brownville is committed to protecting the privacy and security of residents' data and complies with **New York State Technology Law Section 208** regarding breach notification requirements.

II. DEFINITIONS

1. **Personal Information:** Personal data that includes an individual's name, in combination with any one or more of the following: Social Security number, driver's license number, credit or debit card information, or other identifying data.
2. **Security Breach:** Unauthorized access to or acquisition of data that compromises the confidentiality, integrity, or availability of personal information.

III. SCOPE OF APPLICATION

This policy applies to all departments, officials, and employees of the Village of Brownville that handle personal information of residents, employees, or other individuals. It covers all forms of electronic and physical data storage and processing.

IV. NOTIFICATION REQUIREMENTS

1. **When to Notify:**
If a cybersecurity breach results in the unauthorized access or acquisition of personal information, the Village of Brownville must notify affected individuals **without unreasonable delay**. Notification should occur as soon as possible, but no later than **30 days after the breach**.
2. **What to Include in Notification:**
The notification must include the following information:

- A. A description of the breach, including the type of personal information that was involved.
 - B. The date of the breach or approximate date range during which the breach occurred.
 - C. Steps individuals can take to protect themselves, such as monitoring credit reports or placing fraud alerts.
 - D. Contact information for individuals to reach the Village or its designated representative for further questions.
 - E. A statement that the individual can request a credit report or place a fraud alert on their accounts.
3. **Method of Notification:**
- A. **Written Notice:** The preferred method of notification is written notice sent to the individual's last known address.
 - B. **Email Notice:** If the individual has provided their email address to the Village and consented to electronic communication, email may be used.
 - C. **Substitute Notice:** If the Village cannot reach a significant number of affected individuals through written or email notifications, substitute notification methods (such as posting on the Village website or issuing press releases) may be used.
4. **Notification Timeline:**
Notify affected individuals **within 90 days** of discovering the breach. If a delay is unavoidable (due to law enforcement requests, for example), the notification period may be extended, but this should be documented and reported to the Village Board.

V. EXCEPTIONS TO NOTIFICATION REQUIREMENTS

Notification is not required if the Village determines that:

1. **No Personal Information was Compromised:** If the breach only involves data that is not considered personal information under New York law.
2. **Encryption or Masking:** If the personal information involved is properly encrypted, masked, or otherwise rendered unreadable and unusable by unauthorized people.

VI. ADDITIONAL CONSIDERATIONS

1. **Notification to Consumer Reporting Agencies:**
If the breach involves 500 or more individuals, the Village may be required to notify major consumer reporting agencies, such as Equifax, Experian, or TransUnion, about the breach.
2. **Identity Theft Prevention:**
The Village may offer affected individual's resources such as free credit monitoring or identity theft protection services. In cases where there is significant risk of identity theft, the Village should make every effort to help affected individuals mitigate the damage.

3. **Training and Awareness:**

Village staff who handle personal information must be regularly trained on cybersecurity best practices and the breach notification process. This training ensures the Village can quickly respond to incidents and protect residents' data.

VII. ROLES AND RESPONSIBILITIES

1. **Village _____ or Designated Cybersecurity Officer:**

The Village _____ (or designated officer) is responsible for leading the breach response and ensuring compliance with the breach notification requirements. This individual will work with IT professionals and legal counsel to assess the severity of the breach, document its impact, and issue notifications.

2. **Village IT Department:**

The IT Department is responsible for investigating and identifying the cause of the breach, mitigating the risk, and reporting the findings to the Village _____. The IT team should also work to enhance cybersecurity to prevent future incidents.

3. **Village Legal Counsel:**

Legal counsel should be consulted immediately after the breach is discovered to ensure compliance with all legal obligations under **New York State Technology Law Section 208**, and to provide guidance on notification procedures and any potential legal implications.

VIII. RECORD-KEEPING AND DOCUMENTATION

The Village shall maintain comprehensive records of all breaches, including:

- A. The nature and scope of the breach.
- B. The individuals affected.
- C. The notifications sent.
- D. Any actions taken to mitigate harm or prevent future breaches.

These records will be kept for a minimum of **three years** and will be available for review by the Village Board and auditors.

IX. COMPLIANCE AND REVIEW

This policy will be reviewed annually or after any significant cybersecurity breach, to ensure its continued effectiveness and compliance with **New York State Technology Law Section 208** and any other relevant laws or regulations.



PO BOX 118 • 216 BROWN BLVD • BROWNVILLE, NY 13615 • 315-782-7650
CLERK@VILLAGEOFBROWNVILLE.NY.COM • WWW.VILLAGEOFBROWNVILLE.NY.GOV

Cybersecurity Breach Notification Policy
Pursuant to New York State Technology Law Section 208
ADOPTED BY VILLAGE BOARD RESOLUTION _____ OF 2026

I. Purpose

The purpose of this policy is to establish a clear and consistent process for notifying individuals in the event of a cybersecurity breach that compromises their personal information. The Village of Brownville is committed to protecting the privacy and security of residents' data and complies with **New York State Technology Law Section 208** regarding breach notification requirements.

II. Definitions

1. **Personal Information:** Personal data that includes an individual's name, in combination with any one or more of the following: Social Security number, driver's license number, credit or debit card information, or other identifying data.
2. **Security Breach:** Unauthorized access to or acquisition of data that compromises the confidentiality, integrity, or availability of personal information.

III. Scope of Application

This policy applies to all departments, officials, and employees of the Village of Brownville that handle personal information of residents, employees, or other individuals. It covers all forms of electronic and physical data storage and processing.

IV. Notification Requirements

1. When to Notify:

If a cybersecurity breach results in the unauthorized access or acquisition of personal information, the Village of Brownville must notify affected individuals **without unreasonable delay**. Notification should occur as soon as possible, but no later than **30 days after the breach**.

2. **What to Include in Notification:**

The notification must include the following information:

- A. A description of the breach, including the type of personal information that was involved.
- B. The date of the breach or approximate date range during which the breach occurred.
- C. Steps individuals can take to protect themselves, such as monitoring credit reports or placing fraud alerts.
- D. Contact information for individuals to reach the Village or its designated representative for further questions.
- E. A statement that the individual can request a credit report or place a fraud alert on their accounts.

3. **Method of Notification:**

- A. **Written Notice:** The preferred method of notification is written notice sent to the individual's last known address.
- B. **Email Notice:** If the individual has provided their email address to the Village and consented to electronic communication, email may be used.
- C. **Substitute Notice:** If the Village cannot reach a significant number of affected individuals through written or email notifications, substitute notification methods (such as posting on the Village website or issuing press releases) may be used.

4. **Notification Timeline:**

- A. Notify affected individuals **within 90 days** of discovering the breach. If a delay is unavoidable (due to law enforcement requests, for example), the notification period may be extended, but this should be documented and reported to the Village Board.

V. Exceptions to Notification Requirements

Notification is not required if the Village determines that:

- 1. **No Personal Information was Compromised:** If the breach only involves data that is not considered personal information under New York law.

2. **Encryption or Masking:** If the personal information involved is properly encrypted, masked, or otherwise rendered unreadable and unusable by unauthorized people.

VI. Additional Considerations

1. **Notification to Consumer Reporting Agencies:**

If the breach involves 500 or more individuals, the Village may be required to notify major consumer reporting agencies, such as Equifax, Experian, or TransUnion, about the breach.

2. **Identity Theft Prevention:**

The Village may offer affected individual's resources such as free credit monitoring or identity theft protection services. In cases where there is significant risk of identity theft, the Village should make every effort to help affected individuals mitigate the damage.

3. **Training and Awareness:**

Village staff who handle personal information must be regularly trained on cybersecurity best practices and the breach notification process. This training ensures the Village can quickly respond to incidents and protect residents' data.

VII. Roles and Responsibilities

1. **Village Administrator or Designated Cybersecurity Officer:**

The Village Administrator (or designated officer) is responsible for leading the breach response and ensuring compliance with the breach notification requirements. This individual will work with IT professionals and legal counsel to assess the severity of the breach, document its impact, and issue notifications.

2. **Village IT Department:**

The IT Department is responsible for investigating and identifying the cause of the breach, mitigating the risk, and reporting the findings to the Village Administrator. The IT team should also work to enhance cybersecurity to prevent future incidents.

3. **Village Legal Counsel:**

Legal counsel should be consulted immediately after the breach is discovered to ensure compliance with all legal obligations under **New York State Technology Law Section 208**, and to provide guidance on notification procedures and any potential legal implications.

VIII. Record-Keeping and Documentation

The Village shall maintain comprehensive records of all breaches, including:

- A. The nature and scope of the breach.
- B. The individuals affected.
- C. The notifications sent.
- D. Any actions taken to mitigate harm or prevent future breaches.

These records will be kept for a minimum of **three years** and will be available for review by the Village Board and auditors.

IX. Compliance and Review

This policy will be reviewed annually or after any significant cybersecurity breach, to ensure its continued effectiveness and compliance with **New York State Technology Law Section 208** and any other relevant laws or regulations.

This law requires public employers, like the Village of Brownville, to establish policies to ensure compliance with the law during public health emergencies, which includes implementing provisions for paid sick leave, time off for quarantine, and ensuring that workers are not retaliated against for taking leave during such emergencies