Operation Oswego County, Inc.
Data Security Breach Policy and Procedure
Effective Date: 3/9/2020
Last Revised: 1/16/2020

The company considers the unwanted and/or unauthorized release and exposure of personal information collected through the course of its business and operations a serious issue. While it has implemented and maintains policies and procedures to protect this data, the company recognizes the potential risks associated with security breaches. Under certain circumstances, and in accordance with federal and state laws, the company is required to provide notice about data security breaches of protected personal information to affected individuals and appropriate state agencies. In the event that sensitive and/or protected personal information collected by the company is exposed as a result of a Data Security Breach, as defined below, the following procedures MUST and will be followed.

Definition - What does *Data Security Breach* mean?

A Data Security Breach is an incident that involves the unauthorized or illegal viewing, use, access or retrieval of data by an individual, application, or service. It may be a breach specifically designed to steal and/or to publish data to an unsecured or illegal location but can also involve the intentional or inadvertent release of or unauthorized access to data which may compromise the security, confidentiality or integrity of personal information. Data Security Breaches are typically targeted at digital data and conducted over the Internet or a network connection.

A Data Security Breach may result in data loss or release, including financial, personal and health information. A hacker also may use stolen data to impersonate another individual to gain access to a more secure location. For example, a hacker's Data Security Breach of a network administrator's login credentials can result in access to an entire network.

A Data Security Breach may also be known or referred to as a “data spill” or a “data leak”.

Definition - What does *Personal Information* mean?

For purposes of this policy, Personal Information is defined as an individual’s first name or first initial and last name, in combination with any of the following data:

- Social Security number*
- Driver’s license number or government-issued Identification Card number
- Financial account number, credit or debit card number with or without any personal identification number such as an access code, security codes or password that would permit access to an individual’s financial account*
- Account passwords or personal identification numbers or other access code

- Home address or email address
- Medical or health information*
- Biometric data, meaning data generated by electronic measurements of an individual's unique physical characteristics that may be used to authenticate or ascertain the individual's identity, or
- A username or email address in combination with a password or security question that would permit access to an online account.

* Any breach that involves the compromise of data that by itself, and not in combination of any other data, may result in identity theft of an individual will also qualify as Personal Information.

Also note that Personal Information does not include information that is lawfully made available to the general public from federal, state or local government records.

Breach Notification Team

The company has assembled a Breach Notification Team which, in the event of a possible or actual Data Security Breach, is responsible for communicating, investigating and reporting on the Data Security Breach. This Breach Notification Team consists of the following staff members:

- Michael Treadwell, Executive Director (Human Resources)
- Austin Wheelock, Deputy Director and Property Manager/Director of Loss Prevention (Operations and Loss Prevention)
- Evelyn LiVoti, Marketing & Development Manager/Data Security Coordinator (Management Information Systems and Public Relations)
- Barclay Damon, Legal Team

Utilizing the members of its Breach Notification Team, the company will investigate every possible and actual Data Security Breach and report on relevant facts to determine whether it has a duty to notify the public, affected individuals and state agencies of the Data Security Breach, as required by applicable law.

Types of Breaches

There are many types of computer incidents that may require notice to and action by the Breach Notification Team. Some examples include:

- Data Security Breach of Personal Information – either via physical or electronic form
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak
- Ransomware attack

Personal Information Data Security Breach:

The following incidents may require notification to individuals under applicable laws and regulations:

- A user (company associate, contractor, or third-party provider) has, without authorization, used or obtained access to Personal Information maintained in either paper or electronic form.
- An intruder has broken into database(s) that contain Personal Information on any individual or information that is capable of compromising the security, confidentiality, or integrity of Personal Information.
- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing Personal Information on an individual or information that is capable of compromising the security, confidentiality, or integrity of Personal Information has been lost or stolen.
- Paper records containing Personal Information or information that is capable of compromising the security, confidentiality, or integrity of Personal Information, have not been properly disposed of or have been lost or stolen.
- A third party service provider has experienced any of the incidents above, affecting the company's data containing Personal Information.

The following incidents may NOT require individual notification under applicable laws and regulations as long as the company can reasonably conclude after an investigation that misuse of the Personal Information is unlikely to occur and appropriate steps are taken to safeguard the interests of affected individuals:

- The company is able to retrieve Personal Information on an individual that was stolen, and based on its investigation, reasonably conclude that the retrieval took place before the Personal Information was copied, misused, or transferred to another person who could misuse it.
- The company determines that Personal Information on an individual was improperly disposed of, but can establish that the Personal Information was not retrieved or used before it was properly destroyed.
- An intruder accessed files that contain only individuals' names and addresses.
- A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device which has not been compromised.

Investigation

In the event that an associate (i) detects or otherwise learns of a Data Security Breach of either electronic or paper files, (ii) suspects that a Data Security Breach has occurred, or (iii) has any information that may relate in any way to a possible Data Security Breach, all members of the Breach Notification Team should **immediately** be alerted. If the potential breach is electronic in nature, the Data Security Coordinator will begin the investigation to determine where the Data Security Breach occurred, the overall extent of the Data Security Breach and how much data, computers and/or electronic files were affected. This investigation will include, but not be limited to, reviewing firewall, network security application review and server security application review.

To the extent possible, all efforts will be made by the Data Security Coordinator to detect any potential future exposures and prevent further unauthorized access to company data and Personal Information.

Upon isolating where a Data Security Breach of physical records took place, the Director of Loss Prevention should be reviewing surveillance records to determine who had the last access to the area where the Data Security Breach occurred. Security measures such as changed locks and or changed passwords should take place to prevent further unauthorized access to the files and to Personal Information.

Accurate Record Keeping Required

Accurate record keeping will assist in documenting the reasonable and immediate response steps that the company took following notification of a Data Security Breach. Therefore, upon being notified of a potential or actual Data Security Breach, all Breach Notification Team members must keep accurate and contemporaneous notes of all actions taken, by whom, and the exact time and date. Each member of the Breach Notification Team involved in the investigation must record his or her own actions and observations.

The following information, in particular, should be reviewed and recorded:

1. Date, time, duration, and location of the Data Security Breach.
2. How the Data Security Breach was discovered: by whom, and any known details surrounding the Data Security Breach (e.g., method of intrusion, entry or exit points, paths taken, compromised systems, whether data was deleted, modified or viewed, whether any physical assets are missing).
3. Details about the compromised data, including a list of affected individuals and their relationship with the company (associate, vendor, customer, etc.), data fields (including all fields of Personal Information maintained), number of records affected; whether any data was encrypted (if so, which fields). If the data was unencrypted and included an individual's name plus social security number, driver's license or state ID, credit card or bank account information, biometric information, or any username/email address and password/security question that would permit access to an online account, all members of the Breach Notification Team should be notified as soon as possible.

Steps Relating to the Notification of a Data Security Breach Involving Personal Information:

If the Breach Notification Team concludes that the information associated with the Data Security Breach involves Personal Information that was not encrypted or otherwise secured, the following steps are to be followed:

1. If the Data Security Breach relates to electronic records, the Data Security Coordinator should provide a detailed analysis of the nature and extent of the Data Security Breach and the Personal Information compromised in the Data Security Breach. This analysis should determine exactly what Personal Information was breached (i.e. social security numbers) and whether there is a high likelihood that the type of Personal Information compromised could lead to identity theft. The analysis should also, when possible, detail who may have been party to or aware of the disclosure of the Personal Information. This analysis must be in writing.

2. If the Data Security Breach relates to physical records, the Director of Loss Prevention should provide a detailed analysis of the nature and extent of the Data Security Breach and the Personal Information which was compromised in the physical breach. This analysis should include, but not be limited to, which department the physical Personal Information data is/was stored in, who had access to the physical Personal Information data and by what means and the extent to which the physical Personal Information data was protected. The analysis, when possible, should also detail any investigation that has occurred in determining how the physical Data Security Breach took place and to whom the Personal Information may have been disclosed. This analysis must be in writing.

3. Legal Team will need to analyze the legal implications of the Data Security Breach. If necessary, based on the size and/or scope of the Data Security Breach, appropriate authorities (e.g., Attorney General's Office, etc.) may need to be notified per state and federal law. Any notification to individuals may be delayed if law enforcement determines such notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.

4. If the public and/or individuals need to be notified of the Data Security Breach, the Marketing & Development Manager should be notified immediately to allow them time to prepare to answer questions or issue statements, as authorized by the Officers of the company. Notification to media, customer, and/or associates should be prepared, but not sent until first provided to the Legal Team, the Executive Director and at least one Officer of the company for review and authorization to publish.

5. If Notification to individuals is required, it should be timely, conspicuous and delivered in a manner that will ensure the individual receives it. Notice should be consistent with state and federal laws and regulations in content, delivery and timing (generally as soon as practicable).

   Appropriate delivery methods include:
   - Written notice
   - Email notice

- Substitute Notice - Depending on Size and Scope of the Data Security Breach:
- Conspicuous posting of the notice on the company website.
- Notification to major media – subject to prior consent and approval of Executive Director and at least one Officer of the company

Items to consider including in notification to individuals:

- A general description only (no specifics) of the incident and information to assist individuals in mitigating potential harm, including the company's customer service number. An outline of steps individuals can take to obtain and review their credit reports and to file security freeze requests and if necessary, fraud alerts, with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.
- Remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft.
- Inform each individual about the availability of the Federal Trade Commission's (FTC's) online guidance regarding measures to protect against identity theft, and encourage the individual to report any suspected incidents of identity theft to the FTC. Provide the FTC's website address and telephone number for the purposes of obtaining the guidance and reporting suspected incidents of identity theft. http://www.ftc.gov/idtheft. The toll-free number for the identity theft hotline is 1-877-IDTHEFT.

Failure to adhere to this policy and procedure may result in disciplinary action up to and including termination. If an associate has any questions or concerns regarding a Data Security Breach, Personal Information or his or her obligations relating to this policy, please contact the Legal Team, the Executive Director, the Deputy Director, the Marketing & Development Manager or an Officer of the company.

This policy is adopted on the 9th day of March, 2020, by action of the Board of Directors.

_____

Eric Behling
Secretary

Appendix A

The following are selected laws and regulations relating to the breach of personal information about an individual. This Appendix should not be considered a complete list and should annually reviewed for breach law changes and compliance.

Connecticut – CT General Laws Chapter 669, Section 36a-701b

Any person who conducts business in this state and who in the ordinary course of such person's business, owns, license or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security. Notice is not to be unreasonably delayed and in no circumstance later than ninety (90) days after discovery of the breach. Notice is also required to be given to the CT Attorney General at the time the notice is given to any individual.

Maine – Title 10, Part 3 Chapter 210-B, Section 1346

If any person maintains computerized data that includes personal information and becomes aware of a breach to their security system, the person shall conduct a good faith, reasonable and prompt investigation as to the likelihood that personal info has been or will be misused. Notice shall be given of the breach to a ME resident if the personal information has been misused or if it is reasonably possible that the info will be misused. Notice is also required to be given to the ME Attorney General. If notification must be given to more than 1,000 individuals at one time with respect to a security breach, then all major consumer reporting agencies must also be notified.

Massachusetts – MGL c. 93H, Section 3

Notice is required to be given to any resident who may have been affected by a breach of security, or when personal information has been acquired or used by an unauthorized person as soon as practicable and with no unreasonable delay. Notice is also required to be sent to the MA AG and to the Director of Consumer Affairs and Business Regulation through its online portal.

New Hampshire – NH Statutes -Title 31, Chapter 359 –C, Section 359-C:19-21

Any person doing business in NH who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible. Notice is also required to be given to the NH Attorney General. If notification must be given to more than 1,000 individuals at one time with

respect to a security breach, then all major consumer reporting agencies must also be notified.

New Jersey – NJ Statutes – Title 56:8:161-164

Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years. If notification to individuals is required, notification shall be FIRST provided to NJ Division of State Police and the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities. If notification must be given to more than 1,000 individuals at one time with respect to a security breach, then all major consumer reporting agencies must also be notified.

New York – NY General Business Law Section 899

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 must be notified in accordance with provisions of the New York State Breach Law. Entities must also provide written notification to the New York State Department of State, Division of Consumer Protection, New York State Attorney General and the New York State Division of State Police. If notification must be given to more than 5,000 NY residents at one time with respect to a security breach, then all major consumer reporting agencies must also be notified.

Rhode Island – RIGL 11-49.3-4

Any person that stores, owns, collects, possesses, maintains, acquires, uses or licenses data that includes Personal Information shall provide notification of any disclosure of Personal Information, or any breach of the security system, that poses a significant risk of identity theft to any resident of Rhode Island whose Personal Information was or is reasonably believed to have been, acquired by an unauthorized person or entity. Notice shall occur no later than 45 days upon discovery of the breach. If more than 500 Rhode Island residents are affected, the Attorney General and the major credit reporting agencies shall also be notified.

Vermont – 9 V.S.A CH. 62 Section 2430

A person that maintains or possess computerized data containing personally identifiable information of a consumer shall notify a consumer that there has been a security breach no later than 45 days after the discovery or notification of the breach from a third party. Notice shall also be given to the AG within 14 business days of the discovery of the breach or notification to consumers, whichever is sooner. If notification must be given to more than 1,000 individuals at one time with respect to a security breach, then all major consumer reporting agencies must also be notified.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA requires a covered entity to implement policies and procedures to address security incidents. A security incident means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system. Response and reporting implementation requirements include identifying and responding to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. The HIPAA security standards were effective on April 21, 2003. The compliance date for covered entities is by April 21, 2005 and April 21, 2006 for small health plans.