Data Breach Notification Policy

Statement

Bear Island Land Company and Bear Island Surveying (BI) is governed by the notification requirements of Minnesota Statutes §325E.61 DATA WAREHOUSES; NOTICE REQUIRED FOR CERTAIN DISCLOSURES, and §13.055 DISCLOSURE OF BREACH IN SECURITY; NOTIFICATION AND INVESTIGATION REPORT REQUIRED. Accordingly, BI shall provide timely and appropriate notice, as required, when there is reasonable belief that protected personal information held by BI has been compromised by a data breach.

Purpose

The purpose of this policy is to outline how BI will respond to incidents involving data breaches. It will identify and define steps and procedures that will be followed when those breaches occur and will address how affected individuals will be notified as required by the relevant state or federal laws.

Scope

This policy applies to all BI information assets or information assets under the care of BI, and applies to all employees and individuals who interact with, access, or store BI electronic information regardless of storage device, medium, or physical location.

Definitions

Data Breach - An incident of unauthorized access of data in electronic form containing personal information, sometimes also referred to as a "breach of security" or a "breach".

- Protected personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, and does not include information made lawfully available to the general public from federal, State, or local government
- Good faith acquisition of protected personal information by an employee or agent of BI for a legitimate purpose does not constitute a data breach, provided that the personal information is not used for a purpose other than a lawful purpose of BI and is not subject to further unauthorized

Information Technology (IT) Resources - Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, wired and wireless networks, Internet, email, cloud storage, and social media sites.

Technology Incident Response Team (TIRT) - A team or individual BI has contracted with that has the expertise, technical resources, and decision-making capability to coordinate a quick, effective, and orderly response to technology-related incidents.

Minnesota Statutes §325E.61 and §13.055 - If the company becomes aware of a breach of the personal information it collects, but does not own, it shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay,

consistent with the legitimate needs of law enforcement. These statutes provide the following definitions of what constitutes protected personal information:

1. The first name or first initial and last name **in combination with** any one or more of the following data elements, when the data elements are neither encrypted nor redacted:
    - Social Security Number
    - A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify
    - Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial accounts.
    - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
    - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account

Policy

Reporting responsibilities

All individuals affiliated with BI in any capacity, including but not limited to employees, contractors, and visitors, should report suspected or actual data breaches immediately to Kate Davies or Anna Yahnke.

Examples of the types of incidents to report include, but are not limited to:

- Access to BI IT resources by unauthorized individuals
- Evidence of unauthorized access into a system containing private/confidential data
- An unauthorized attempt to physically enter or break into a secure IT area
- Unauthorized sharing of BI IT login credentials.
- Loss of a BI hardware resource such as laptop, tablet, cell phone, or removable data storage devices.
- Hacking or defacing of a BI online resource
- Documents containing private/confidential data sent in any form to a wrong recipient.
- Employee misuse of authorized access to disclose or mine private or confidential data.

5.2 Activating the Technology Incident Response Team

Upon receipt of a suspected information security breach, BI will convene the Technology Incident Response Team (TIRT) without undue delay to expeditiously conduct a fact-finding investigation to determine whether a data breach or compromise has occurred.

5.3 Security Breach Initial Procedures

Containment - If the TIRT determines there was a data breach, the TIRT will partner with the affected resource to contain the breach.

Assessment - Once the breach is contained and eradicated, the TIRT will assess the extent and impact of the breach.

Data preservation - All evidence related to the breach will be preserved for future analysis.

Documentation - Each step related to the breach and breach investigation will be fully documented.

Reporting and legal obligations - BI will be required to make certain materials available to the state government upon request, such as remedial procedures, incident reports, and computer forensic data.

Notification to Victims

Timing for Providing Notification

Notice must be given when there is discovery or notification of a breach of security of the system. Notice must be given without unreasonable delay. If the breach affects more 500 (1,000 for state agencies), then consumer reporting agencies must be notified within 48 hours.

Notification shall be delayed, however, if a law enforcement agency informs BI that disclosure of the breach would impede a criminal investigation or jeopardize national or homeland security. A request for delayed notification must be made in writing or documented contemporaneously by BI in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The required notification shall be provided without unreasonable delay after the law enforcement agency communicates to BI its determination that notification will no longer impede the investigation or jeopardize national or homeland security.

Responsibility for Providing Notification

BI will assign a person to provide notification as soon as possible after the breach has occurred.

5.4.3 Contents of the Notification

There is no specific statutory requirement as to the content of the notification. However, BI will provide the following information:

- A description of the incident in general terms and a timeline of the data breach.
- A description of the type of personal information that was subject to possible unauthorized access and acquisition.
- A description of the actions taken by BI to protect the personal information from further unauthorized access.
- A telephone number that affected individuals may call for further information as well as directions for the person to remain vigilant by reviewing account statements and monitoring free credit reports.
- The toll-free numbers and addresses for the major consumer reporting agencies.
- Beyond notification and except where required by law, BI makes no promise of service to individuals affected by a data breach. BI, however, may elect to provide additional services to affected individuals at its discretion.

5.4.4 Methods of Notification

- Written notice by first class mail to each affected individual
- or
- Electronic notice to each affected individual if communication normally occurs in that medium

- or
- Telephonic notification provided that the contact is made directly with the affected person(s).
- Substitute notice may be provided if the affected class of individuals to be notified exceeds 500,000, or BI does not have sufficient contact information to notify affected individuals. Substitute notice consists of all of the following:
    - Conspicuous posting of the notice on the institution website for a minimum of 45 days
    - and
    - Notification to major media outlets that reach the general public.
- Whenever notice of data breach is given to more than 500 persons, BI will notify, without unreasonable delay, all three major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

IT Responsibilities

All entities that collect customer data should "take reasonable measures to protect and secure data in electronic form containing personal information" on individuals. BI will be responsible, either internally or through a contracted party, to provide the following:

- Training employees on steps to take to ensure data security as part of their job duties.
- Limiting employees' access to data that each specific employee needs to complete their job requirements.
- Regularly auditing file access permissions.
- Implement procedures for reporting data breaches or violations of security protocol.
- Educating employees on any new developments in data breach security.
- Hiring a security expert to periodically review the security of BI data.
- Implementing disposal standards for customer data no longer to be retained.
- Implementing a yearly practice exercise of this policy and adjusting as necessary.