Data Breach Response Policy

Process Owner: Rob Fea
Created: 6/28/2016
Last Update: 3/1/2019
Last Update By: Rob Fea

Scope

This policy covers all computer systems, network devices, and any additional systems and outputs containing or transmitting Extract's or Extract's customers' protected or sensitive data.

Purpose

The purpose of this policy is to ensure that all necessary parties are notified if and when there has been a security breach while sensitive information is in Extract's possession.

NOTE: For Extract's customers, any additional steps required and agreed upon in the BAA will also be followed and adhered to in addition to the process outlined below.

Team

The Data Breach Response Team (DBRT) consists of the following team members:

Role	Name	Cell Phone	Email
Process owner	Rob Fea	937-248-3668	Rob_Fea@extractsystems.com
Information Security	Steve Kurth	312-813-8809	Steve_Kurth@extractsystems.com
Legal	David Rasmussen	608-347-0477	David_Rasmussen@extractsystems.com
Admin	Lori Owens	608-206-4896	Lori_Owens@extractsystems.com

Policy

Determining if Notification is Needed

The process owner, in consultation with the DBRT, is responsible for determining whether a breach of information security has occurred and whether notification is required. If a breach has or has likely happened, the priority is to limit the negative results which will influence Extract's response. If the data in question is the property of a client, the notification will not be to the individuals, but rather back to the client with an itemized list of information that was compromised. Notification will occur within 24 hours of discovery of the breach.

Notification Process

The DBRT works with responsible employees and others as appropriate to deliver timely and effective notification to those impacted.

1. **Draft the content of notification.**

   While the content may vary, notification must always include these elements, to the extent possible:

   - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
   - A description of the types of private information that were involved in the breach (e.g., full name, social security number, medical record number, date of birth, home address, account number, etc.)

- Any steps individuals should take to protect themselves from possible harm resulting from the breach (e.g., identity theft)
- A brief description of what Extract is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches
- Contact information for further questions and assistance, including a telephone number, an email address, Website address, and/or postal address

2. **Determine the manner of notification**.

   The DBRT determines the appropriate manner of notification:

   - For clients: notification will always be via a phone call followed by an email and delivery of any relevant information needed to take appropriate action.
   - For employees/others: phone call, first-class mail, or email—as required under the law.

3. **Review the notification.**

   All notifications must be reviewed and agreed upon by all members of the DBRT before being sent.

4. **Determine if other actions are required.**

   The DBRT in conjunction with the customer (if applicable) must collectively determine whether other requirements apply, depending on the nature of the information that is the subject of the breach, as well as the scope of the breach.