*Data Breach Response*

*Policy*

### Table of Contents

[Purpose 1](#_Toc4679030)

[Scope 1](#_Toc4679031)

[Policy Statements 1](#_Toc4679032)

[Privacy Breach Preparation and Organization 1](#_Toc4679033)

[Privacy Breach Impact Analysis 2](#_Toc4679034)

[Third-Party Reporting 2](#_Toc4679035)

[Customer Notification 2](#_Toc4679036)

[Media Notices 3](#_Toc4679037)

[Legal Notification 3](#_Toc4679038)

[Remediation Activities 3](#_Toc4679039)

[Violations 4](#_Toc4679040)

[Roles and Responsibilities 4](#_Toc4679041)

[Terms and Definitions 4](#_Toc4679042)

[References 5](#_Toc4679043)

[Related Documents 5](#_Toc4679044)

[Approval and Ownership 5](#_Toc4679045)

[Revision History 6](#_Toc4679046)

Purpose

The purpose of this document is to define CompanyX (the “Company”)policies for responding to potential breaches of sensitive information. This policy is focused on the specific types of security incidents that may involve the accidental disclosure of personally-identifiable information (PII) to unauthorized Third-Parties.

Scope

This policy applies to all CompanyX employees and Third-Party contractors that collect, process or otherwise handle sensitive personal information of employees or customers.

Policy Statements

Privacy Breach Preparation and Organization

**Privacy Breach Response Team** – CompanyX must establish and staff a special team with the responsibility of planning for, analyzing and responding to data breaches. The team must be composed of qualified individuals from various department including (but not limited to) Information Security, Legal, Human Resources, Marketing/PR.

**Privacy Breach Response Plan** – CompanyX must establish and maintain a written Privacy Breach Response Plan detailing the requirements of the response program. The plan must include the names and contact information of specific individuals required to implement the plan, as well as detailed standards and procedures for implementing official breach response policies.

Privacy Breach Impact Analysis

**Security Incident Analysis** – Each security incident reported to the CompanyX Computer Emergency Response Team (CERT) that involves the possible disclosure of sensitive personal information (PII) of employees or customers must be analyzed to determine the event qualifies as a breach under CompanyX standards.

**Breach Notification Analysis** – Each security event identified as a breach must be further analyzed to determine the notification requirements for the breach. Breaches that trigger the notification requirements must be logged and reporting immediately to the Privacy Breach Response Team.

Third-Party Reporting

**Third-Party Reporting System** - CompanyX must establish a formal reporting mechanism to allow Third-Parties that process sensitive personal information to report a breach of such information. CompanyX Computer Incident Response Team members will respond with 24 hours of such notification.

Customer Notification

[Note: Each organization should verify the possible notification methods available to them given their legal requirements. In the majority of cases, written notification is required.]

**Acceptable Notification Methods** – CompanyX must use any one or more of the following methods to notify customers in the event of a data breach:

(1) Written Letter via First Class Mail to the last known address of the individual;

(2) Electronic Mail to the last know electronic mail address,

(3) Personal phone call (only in cases of extremely high risk of identity theft)

**Web Site Notice** – CompanyX must post notice of the privacy breach on the public web site, including details of the breach approved for public disclosure by the Privacy Breach Response Team.

**Timeliness of Notification** – All official customer notifications must be made within 60 days of the discovery of the breach by CompanyX.

[Reference: HITECH Act - (2) BURDEN OF PROOF- The covered entity involved (or business associate involved in the case of a notification required under subsection (b)), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.]

**Record of Notification** – CompanyX must keep a record of each customer notification attempt, including the individual, date, time and notification method.

**Content of Notification** – Regardless of the method by which notice is provided to individuals, notice of a breach must include, to the extent possible, the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of PII that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
3. The steps individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Media Notices

**Media Notice** – If the number of individuals affected by the breach is over 500 individuals within a given state or jurisdiction, then notice of the breach must be disclosed to prominent media within seven days of the breach discovery.

**Media List of Contacts** - A list of media outlets and their appropriate contact information will be maintained by the Legal Department and Marketing Department as part of the breach notification plan.

(Note: Some laws require specific detailed to be included in the notice. This section should be modified based on the organizations specific requirements.)

Legal Notification

**Exception in the Case of Investigation** – The notification requirements of this policy may be suspended if they are found to impede a criminal investigation. This exception must be requested by law enforcement and approved by CompanyX management.

**Reporting to Governing Bodies** – If the discovered breach triggers the Governing Body Reporting Requirement, CompanyX must immediately report details of the breach to the appropriate jurisdiction or legal entity that requires such notice. A list of governing bodies for each law requiring a breach notification must be maintained by the Legal Department, as well as the proper forms required for such a breach.

**Reporting Requirements** – To facility the timely reporting of breaches to governing bodies, The Privacy Breach Response Team must maintain a list of forms required to report the breach to various legal entities or jurisdictions.

Remediation Activities

**Dedicated Support Line** – As part of the breach notification and remediation plan, CompanyX will maintain a dedicated support line to handle customer inquiries regarding the breach. The support line will include an email address and toll-free telephone number. Each support person must be trained in the remediation options available to customers.

**Breach Incident Review** – The Information Security Department must review the details of any privacy breach recorded by CompanyX, even if the incident did not trigger a public announcement. The review must include a detailed analysis of what lead to the breach and a recommended set of updates to existing controls to mitigate the risk of any further breaches.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Roles and Responsibilities

**Management** - Each organizational unit head is responsible for ensuring proper security and protection for all personally identifiable information (PII) within her or his purview.

**Privacy Breach Response Team** – This group is responsible for the planning, analyzing and responding to data breaches.

**Information Security Department** – This group is responsible for formulating, policies, procedures and standards for the security of sensitive personal data. The Information Security Department is also responsible for developing training for employees on the various types of security incidents that may trigger a data breach.

**Marketing/PR Department** – The Marketing Department, with the help of the Privacy Breach Response Team, is responsible for maintaining a list of media outlets and contact information in the event that media must be notified of a breach.

**Legal Department** – The Legal Department is responsible for identifying, with help of the members of the Breach Response Team, the various breach reporting requirements for each jurisdiction in which CompanyX handles personally identifiable information (PII).

**Employees and other users** – Each user entrusted with that processes or handles PII is responsible for following the information protection policies designed to protect this information. Individuals are also responsible for notifying management if they suspect that a breach of such notification may have occurred.

Terms and Definitions

**Breach Discovery** – A data breach is considered “discovered” within 24 hours of its initial report and when the “notification clause” has been triggered.

[REF: HITECH…, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.]

**Governing Body Notification Requirement** – A privacy breach found to contain PII that requires reporting to the regulatory agency or other governing body will trigger this notification requirement.

**Notification Requirement** – A data breach of sensitive personal information that is found to be reasonably likely to result in identify theft will trigger a Notification Requirement.

**Notification Burden of Proof** - The requirement to demonstrate that all required notifications were made in response to a privacy breach.

**Privacy Breach** - A privacy breach occurs when personal information is collected, retained, accessed, used, or disclosed in ways that are not in accordance with the provisions of the enterprise’s policies, applicable privacy laws, or regulations.

**Privacy Breach Response Team** – A special multi-disciplinary team that is responsible for planning, analyzing and responding to privacy breaches. The team will be composed of qualified individuals from various department including (but not limited to) Information Security, Legal, Human Resources, Marketing/PR.

(Note: Organizations must modify this definition to match the various types of PII collected.)

**Personally Identifiable Information (PII)** –Information that alone, or when combined with other personal or identifying information can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

**Privacy-Applicable Law** –Relevant laws, enactments, regulations, binding industry codes, regulatory permits and licenses that are in effect and address the protection, handling and privacy of target privacy data.

**Sensitive personal information** - Personal information that requires an extra level of protection and a higher duty of care, for example, information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

References

HITECH Act SEC. 13402. NOTIFICATION IN THE CASE OF BREACH.

AICPA/CICA Generally Accepted Privacy Principles

CA SB 1386

General Data Protection Regulation (GDPR)

UK - Data Protection Act (DPA)

FACTA – Red Flags Rule

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |