Data Breach Response Policy

Defines the goals and the vision for the breach response process. This policy defines to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms.

Last Update Status: 27 Nov*, 2016*

1. Overview

This policy mandates that any individual who suspects that a theft, breach or exposure of BuildWealth Technologies Pvt Ltd Protected data or BuildWealth Technologies Pvt Ltd Sensitive data has occurred must immediately provide a description of what occurred via e-mail to corp@wealthy.in. This e-mail address is monitored by the BuildWealth Technologies Pvt Ltd's Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2. Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

BuildWealth Technologies Pvt Ltd Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how BuildWealth Technologies Pvt Ltd's established culture of openness, trust and integrity should respond to such activity. BuildWealth Technologies Pvt Ltd Information Security is committed to protecting BuildWealth Technologies Pvt Ltd's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

3. Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information(PII) or Protected Health Information (PHI) of BuildWealth Technologies Pvt Ltd members.

4. Policy

4.1 As soon as a theft, data breach or exposure containing BuildWealth Technologies Pvt Ltd Protected data or BuildWealth Technologies Pvt Ltd Sensitive data is identified, the process of removing all access to that resource will begin.

The Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Director

Confirmed theft, breach or exposure of BuildWealth Technologies Pvt Ltd data

The Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by BuildWealth Technologies Pvt Ltd cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan

Work with BuildWealth Technologies Pvt Ltd communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

4.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the BuildWealth Technologies Pvt Ltd community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any BuildWealth Technologies Pvt Ltd Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

- Information Security Administrator is that member of the BuildWealth Technologies Pvt Ltd community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

- Users include virtually all members of the BuildWealth Technologies Pvt Ltd community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.