SCIGON
Technology Consulting | Engineering | Products

Data Breach Response Policy/Procedures

Contents

Response Team 1
Purpose 1
Background 2
Scope 2
Current State 2
Policy on storage and/or processing of personally identifiable information, Protected Health Information (PHI) and/or proprietary data of SCIGON and/or its customers and partners 2
Personally identifiable information or Protected Health Information (PHI) of SCIGON's personnel and Proprietary Data 2
Personally identifiable information, Protected Health Information (PHI), and Proprietary Data of SCIGON's customers and partners 3
Policy on Confirmed theft, data breach or exposure of SCIGON Protected data or SCIGON Sensitive data 3
Work with Forensic Investigators 3
Develop a communication plan. 3
Ownership and Responsibilities 4
Roles & Responsibilities: 4
Enforcement 4
Definitions 4

Response Team

Name	Roles	Emails	Office/Mobile
John Scifers	CEO/Chief Technologist/Response Team Lead	jscifers@scigon.com jscifers@gmail.com	847-453-8890 630-544-9798
Eugene Gonchar	COO/Response Team Lead Backup	egonchar@scigon.com egonchar@hotmail.com	847-453-8885 224-212-0505

Purpose

The purpose of the policy is to establish the breach response process and associated policy. This document 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 made easily available to all personnel whose duties involve data privacy and security protection.

SCIGON Solutions' ("SCIGON") intentions for publishing a Data Breach Response Policy/Procedures is to focus significant attention on data security and data security breaches and how SCIGON's established culture of openness, trust and integrity should respond to such activity. SCIGON is committed to protecting SCIGON's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Background

This policy mandates that any individual who suspects that a theft, breach or exposure of SCIGON Protected data or SCIGON Sensitive data has occurred must immediately provide a description of what occurred via e-mail to helpdesk@SCIGON.com, or by calling 877-554-5678. This e-mail address is monitored by SCIGON's Response Team Lead. The appropriate 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 Response Team Lead will follow the appropriate procedure in place.

Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of SCIGON and/or its customers and partners.

Current State

SCIGON does not store, process or otherwise handle personally identifiable information, Protected Health Information (PHI), or other sensitive data for any partner or customer. Personally identifiable information or Protected Health Information (PHI) of SCIGON personnel, and sensitive company data, is stored in an encrypted format in systems to which only SCIGON's management team has access.

Policy on storage and/or processing of personally identifiable information, Protected Health Information (PHI) and/or proprietary data of SCIGON and/or its customers and partners

Personally identifiable information or Protected Health Information (PHI) of SCIGON's personnel and Proprietary Data

- Personally identifiable information or Protected Health Information (PHI) of SCIGON's personnel shall be stored only in an encrypted electronic format in secure, cloud-based servers (e.g. Intermedia Exchange/SharePoint).
- Paper documents such as facsimiles containing such personally identifiable information or Protected Health Information (PHI) shall immediately be converted to electronic format and stored in an encrypted format in secure, cloud-based servers (e.g. Intermedia Exchange/SharePoint). The paper version of such documents should then be shredded using SCIGON's paper shredder.
- No documents containing personally identifiable information or Protected Health Information shall be stored on portable media (e.g. USB drive, CD, etc.) at any time
- Proprietary and sensitive company documents and data shall be stored only in an encrypted electronic format on Cloud-based storage solutions to which only SCIGON management personnel have access.
- Only SCIGON's management team shall have access to such personally identifiable information, Protected Health Information (PHI) and proprietary SCIGON data.
- Such personally identifiable information or Protected Health Information (PHI) shall only be used for legitimate business purposes. In the event that personally identifiable information or Protected Health Information (PHI) must be used for business purposes (such as background check, managing health

benefits, etc.), the subject of that information shall provide permission for use of that information, and only within the scope of that activity (e.g. background check, obtaining health benefits, etc.).

Personally identifiable information, Protected Health Information (PHI), and Proprietary Data of SCIGON's customers and partners

- SCIGON shall not process, transmit, accept or store personally identifiable information, Protected Health Information (PHI), or other sensitive data of its customers and partners using SCIGON facilities or equipment, unless mutually agreed to in advance.
- In the event that SCIGON is asked by a partner or customer to process, transmit, accept or store personally identifiable information, Protected Health Information (PHI), or other sensitive data using SCIGON facilities or equipment, SCIGON and the partner or customer will agree to appropriate means for the storage, transmission and/or processing of such data, as well as the development of appropriate policies for handling that information.

Policy on Confirmed theft, data breach or exposure of SCIGON Protected data or SCIGON Sensitive data

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

The Response Team Lead will assemble an incident response team to handle the breach or exposure.

The team will address, as applicable:

- IT Infrastructure
- IT Applications
- Finance
- Legal
- Communications
- 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

The incident response team will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As appropriate, Response Team will engage forensic investigators to 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.

Response Team will work with SCIGON communications, legal and human resource resources to decide how to communicate the breach to: a) internal employees, b) external stakeholders, and c) those directly affected.

Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those personnel of SCIGON that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any SCIGON Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Response Team Lead is that employee of SCIGON 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 SCIGON personnel to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

Enforcement

Any SCIGON personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their relationship terminated.

Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;
Plain text – Unencrypted data.
Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).
Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered
Protected data - See PII and PHI
Information Resource - The data and information assets of an organization, department or unit.
Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.