13701 NE Bel-Red Rd, Suite 103
Bellevue, WA 98005
https://www.perimatics.com

DATA BREACH RESPONSE POLICY

1. 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.

Perimatics 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 Perimatics's established culture of openness, trust and integrity should respond to such activity. Perimatics Information Security is committed to protecting Perimatics's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of Perimatics Protected data or Perimatics Sensitive data has occurred must immediately provide a description of what occurred via e-mail to infosec@Perimatics.com, or by calling 425-298-0956. This e-mail address and phone number are monitored by the Perimatics'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. 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 Perimatics members. Any agreements with vendors will contain language similar that protects the organizations involved.

3. POLICY CONFIRMED THEFT, DATA BREACH OR EXPOSURE OF PERIMATICS PROTECTED DATA OR

PERIMATICS SENSITIVE DATA

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

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

The team will include members from:

- IT Infrastructure
- 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 by the Executive Director

Confirmed theft, breach or exposure of Perimatics data

The CTO and CEO 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 Perimatics 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 Perimatics 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. Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the Perimatics community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Perimatics 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 Perimatics community, designated by the COO, 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 Perimatics 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 the COO and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, Communications, Legal, Management, and Human Resources.

5. Enforcement

Any Perimatics 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 network connection terminated.

6. Revision History

Date of Revision	Author	Description of Changes
Jan 2019	COO	Initial version; format changed