Data Breach Notification Policy

Version 1 - Approved by Shreyas Srinivas

Contents

1. Objective

The objective of this policy is to outline the guidelines for notifying individuals, regulatory authorities, and other relevant parties in the event of a data breach. The policy aims to ensure prompt and appropriate actions are taken to mitigate the impact of a data breach, uphold the privacy and security of individuals' data, and comply with applicable laws and regulations.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who handle personal information in the course of their work for our organization.

3. Policy Statement

At Inai Technologies Co, we are committed to safeguarding the data that we collect for the delivery of our services. If sensitive data is acquired, accessed, used, or disclosed in a manner not permitted under the privacy law or in a manner that compromises the security or privacy of the sensitive data(personal data or PHI), it may be considered a Breach.

Data breach notification procedures shall be created to define procedures and responsibilities to ensure a quick, effective, consistent, and orderly response to Information Security Incidents which lead to a Data breach.

4. Reporting of Suspected Breach

Any Inai Technologies Co staff member who discovers a potential breach of sensitive data shall report it to the company’s Information Security Officer immediately.

5. Investigation of Suspected Breach

The Information Security Officer shall review the circumstances of the suspected breach to determine if the incident was intentional or unintentional. Certain unintentional incidents described more fully below, do not constitute reportable breaches.

1. If sensitive data was acquired, accessed, or used by a staff member of Inai Technologies Co, but the acquisition, access, or use was made in good faith and within the scope of permitted activities of the staff member, and there is no further unpermitted use or disclosure, then this does not constitute a breach.

2. If sensitive data was inadvertently disclosed by one staff member of Inai Technologies Co to another staff member, and there is no further unpermitted use or disclosure, then this does not constitute a breach.

3. The Information Security Officer shall review the circumstances of the suspected breach to determine if the incident poses a significant risk of financial, reputational, or other harm to the customer. The risk assessment shall be documented. If the risk assessment results in a conclusion that the incident could cause a significant risk of harm, notification will be made as described in the Breach Notification section below.

6. Breach Notification to the customer

In the case of a sensitive customer data breach, the Information Security officer shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the authority competent in accordance with laws governing the contract, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Mitigation

Inai Technologies Co shall mitigate, to the extent practicable, any harmful effect that is known to the company of a use or disclosure of sensitive data in violation of its business associate agreements.

7. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

8. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

9. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

10. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Data Breach Notification Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Shreyas Srinivas	12 Mar, 2024
1	New Policy version Created	12 Mar, 2024