DATA BREACH POLICY

1. Purpose

This policy describes how Hellenic.me will respond to a data breach, in adherence to the Privacy Act 1988.

It is Hellenic.me's belief that clear roles, responsibilities and procedures will serve as the foundation as a comprehensive privacy program.

This policy outlines:

(a) the steps that Hellenic.me will take to contain, assess, notify, and review any data breaches that might occur; and
(b) Notifiable Data Breaches and how Hellenic.me will address them if they occur.

All Hellenic.me employees, officers, representatives or advisers ('Employees') are required to understand and act in accordance with this policy.

2. Data Breach Definition

A data breach occurs when personal information or intellectual property held by Hellenic.me is subject to unauthorised access, disclosure, modification, or is lost. Data breaches can occur in a number of ways, including but not limited to:

(a) Unauthorised Third-party security breaches (e.g. Hackers)
(b) Unauthorised access, disclosure or modification by Employees and users
(c) Data breaches of Third-party services used by Hellenic.me that affect user data

Specific to Hellenic.me's business, the following have been identified as possible data breach sources:

(a) Accidental loss, unauthorised access, or theft of classified material data or equipment on which such Hellenic.me data is stored, such as company Laptops and USBs.
(b) Unauthorised use, access to, or modification of data on Hellenic.me's Standard Servers.
(c) Accidental disclosure of Hellenic.me user data or intellectual property, such as via email to an incorrect address.
(d) Unauthorised data collection by third parties posing as Hellenic.me, e.g. Phishing Scam
(e) Failed or successful attempts to gain unauthorised access to Hellenic.me information or information systems
(f) Unauthorised data collection by third parties through Malware infections on Hellenic.me cloud databases, or hardware equipment.

3. What to do if a Data Breach is Suspected?

All Hellenic.me Employees who are aware of, informed of, or suspect a data breach must inform Hellenic.me's IT team immediately. The IT team must then assess the suspected breach to determine whether or not a breach has in fact occurred. If a data breach has, in fact, occurred, then the IT team will manage the breach according to the steps outlined in the Data Breach Management Plan.

4. Data Breach Response Plan

In accordance with OAIC recommendations, the following steps will be taken in response to a verified Data Breach.

(a) Contain the breach as soon as possible. Containment is ensuring that the breach itself is stopped. How a breach is stopped would depend on the particular instance but can include:
   (i) The suspension of compromised accounts;
   (ii) Removal of malware, where identified;
   (iii) Temporary platform downtime if necessary;
   (iv) Recovering any lost data, if possible;
   (v) Repairing unauthorised modification of data, if possible;
   (vi) Restoring access to the platform when able.

(b) Assess the risks involved and the repercussions on respective stakeholders. The following may be considered in assessing the stakeholder risks:
   (i) The type of information involved;
   (ii) Establish the cause and the extent of the breach;
   (iii) Assess the risk of harm to affected persons;
   (iv) Assess the risk of other harms: reputational damage;
   (v) Notify Management and Affected Individuals where appropriate;
   (vi) Management must be notified of breaches as and when they occur, whether or not the breach is an eligible breach under the Notifiable Data Breach Scheme;
   (vii) Hellenic.me is an APP 11 entity under the Privacy Act 1988 (Cth) and is and must, therefore, comply with its obligations under the Notifiable Data Breach Scheme;
   (viii) Data Breaches that are not eligible under the Notifiable Data Breach Scheme need not be reported and may be addressed internally.

(c) Prevent future similar breaches through strengthening security infrastructures and/or policies

5. Notifiable Data Breach Scheme

Under the Notifiable Data Breach Scheme, Hellenic.me is obliged to report data breaches that satisfy the following criteria:

(a) there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that Hellenic.me holds;
(b) That the unauthorised access to or disclosure of, or loss of personal information is likely to result in serious harm to one or more individuals; and
(c) Hellenic.me has not been able to prevent the likely risk of serious harm with remedial action.

For further information on how to assess a notifiable data breach, Hellenic.me must refer to the OAIC's APP guidelines.

Where Hellenic.me suspects that an eligible breach has occurred, it must carry out a reasonable and expeditious assessment of the breach: s 26WH(2)(a) of the Privacy Act. Where possible, the assessment must be completed within 30 days of Hellenic.me becoming aware of information that causes it to suspect that an eligible breach has occurred. If Hellenic.me is unable to complete the assessment within 30 days, a written document must be written which addresses:

(a) how all reasonable steps have been taken to complete the assessment within 30 days;
(b) the reasons for the delay; and
(c) that the assessment was reasonable and expeditious.

Where an Eligible Breach has occurred, Hellenic.me must inform affected users AND the Privacy Commissioner. Hellenic.me is allowed to disclose eligible breaches to users in either of the following ways:

(a) It may notify all Hellenic.me users
(b) It may notify affected Hellenic.me users
(c) It may publish a notification on its website

Disclosure of eligible breaches to the Privacy Commissioner may be done by online form.

For more information on disclosing Eligible Breaches under the Notifiable Data Breach Scheme, please refer to the OAIC's webpage on the topic.

6. Disciplinary Consequences

Hellenic.me reserves the right to monitor Employees' use, access and modification of the company's data, and initialise an investigation if cases where an employee conducts an action that is in breach of this policy.

All Employees should handle Hellenic.me's data with due diligence in accordance with this policy and any related policies. If an employee's action or omission that is prohibited under this policy causes a disruption of integrity to the data system or leads to a breach defined in the Privacy Act, the employee may face severe disciplinary action up to and including termination at the discretion of Hellenic.me.