DATA BREACH POLICY

Heavy Industry Low-carbon Transition CRC (HILT CRC)
ACN 652 464 796

1. Purpose

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

It is HILT CRC'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 HILT CRC will take to contain, assess, notify, and review any data breaches that might occur; and

(b) Notifiable Data Breaches and how HILT CRC will address them if they occur.

All HILT CRC employees, officers and representatives are required to understand and act in accordance with this Policy.

The Chief Operating Officer is to ensure that the external IT service provider understands and acts in accordance with this Policy and that this is reflected in the services agreement in so far as is reasonably practicable.

2. Data Breach Definition

A data breach occurs when personal information or intellectual property held by HILT CRC 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 HILT CRC that affect user data

Specific to HILT CRC'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 HILT CRC data is stored, such as company Laptops and USBs.

(b) Unauthorised use, access to, or modification of data on HILT CRC's Project Management System 'HILT Hub'

(c) Accidental disclosure of HILT CRC user data or intellectual property, such as via email to an incorrect address.

(d) Unauthorised data collection by third parties posing as HILT CRC, e.g. Phishing Scam

(e) Failed or successful attempts to gain unauthorised access to HILT CRC information or information systems

(f) Unauthorised data collection by third parties through Malware infections on HILT CRC cloud databases, or hardware equipment.

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

Any HILT CRC employee, officer or representative who is aware of, informed of, or suspects a data breach must inform HILT CRC's Chief Operating Officer immediately who will in turn notify HILT CRC's external IT service provider.

The external IT service provider is responsible for notifying HILT CRC's Chief Operating Officer immediately should it be aware of, informed of, or suspects a data breach.

The Chief Operating Officer, working with the external IT service provider, 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 Chief Operating Officer will manage the breach according to the steps outlined in the Data Breach Response Plan.

4. Data Breach Response Plan

In accordance with OAIC recommendations https://bit.ly/43KIWUa, 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) HILT CRC is an APP 11 entity under the Privacy Act 1988 (Cth) 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, HILT CRC 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 HILT CRC 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) HILT CRC 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, HILT CRC must refer to the OAIC's APP guidelines https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines

Where HILT CRC 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. HILT CRC must take all reasonable steps to ensure that the assessment is completed within 30 days of becoming aware of information that causes it to suspect that an eligible breach has occurred. If HILT CRC 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, HILT CRC must inform affected users AND the Privacy Commissioner. HILT CRC is allowed to disclose eligible breaches to users in either of the following ways:

(a) It may notify all HILT CRC users

(b) It may notify affected HILT CRC 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

HILT CRC 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 HILT CRC'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.

7. Other Company Policies

This Policy must be followed in conjunction with the following related Company Policies which can be found on the Company's website:

(a) Cyber Security Policy

(b) Privacy Policy

8. Review

The Company will review this policy annually and update as required to ensure the continued security of the Company. It is important for those to whom this policy applies to stay up-to-date with changes to this policy, as this is a rapidly-changing area.

Version 1
Approved by HILT CRC Board 18 April 2024