HILTCRC

CYBER SECURITY POLICY

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

1. Intent and Scope

(a) This cybersecurity policy (**Policy**) provides the basis of cybersecurity management within HILT CRC (**Company**).

(b) This Policy applies to HILT CRC employees, employees of HILT CRC Partners, HILT's external IT service provider(s) and anyone else who may have any type of access to the Company's systems, software, hardware, data and/or documents (collectively referred to as the **Participants**).

(c) Effective protection of business information creates a competitive advantage, both in the ability to preserve the reputation of the Company and in reducing the risk of the occurrence of negative events and incidents.

(d) This policy aims to balance the following priorities:

(i) Meeting the Company's legislative requirements.

(ii) Keeping data and documents confidential as required by the Company and its stakeholders.

(iii) Ensuring the integrity of the Company's data and IT systems.

(iv) Upholding the Company's reputation as a trusted recipient of data.

(v) Maintaining storage and back-up systems that meet the needs of the Company and its Participants.

2. Responsibilities

(a) This policy applies to all Participants who are given access to the Company's systems, software, hardware, data and/or documents.

(b) All Participants are responsible for protecting business information and systems. Where there is any doubt about the security of any action, the Participants should take a cautious approach and avoid any potential risks.

(c) HILT CRC is responsible for taking all reasonable steps to establish and maintain a secure IT environment for its Participants on behalf of all stakeholders.

(d) HILT CRC's external IT service provider will provide the necessary support as per their service agreement with HILT CRC and will follow the process defined within the HILT CRC Data Breach Policy.

(e) HILT CRC's external IT service provider is responsible for establishing and maintaining security controls that follow the ASCS Essential Eight guidelines, at Maturity Level 2 (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model)

(f) The Chief Operating Officer is responsible for implementing this policy.

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

3. Authorisation and Access

Managers should exercise caution when:

- Sharing information and documents with the Participants.
- Authorising the Participants to enter and control information systems.
- Giving the Participants access to information systems.

As a general rule, managers should follow a need-to-know basis. If there is any uncertainty regarding how information and documents should be shared, contact the Chief Operating Officer at HILT CRC.

4. Password and Authentication Requirements

(a) To avoid the Participants' work account passwords being compromised, these best practices are advised for setting up passwords:

(i) Passwords set up by an administrator must be uniquely and randomly generated, then immediately changed by the user.

(ii) Use at least 8 characters (must contain capital and lower-case letters, numbers and symbols).

(iii) Do not write down password and leave it unprotected.

(iv) Do not exchange credentials when not requested or approved by supervisor.

(b) Change passwords when there is any possibility that an existing password may have been compromised.

(c) We encourage the use of a password management tool, whether integrated into a mobile app or an internet browser.

(d) Multifactor authentication tools should be used where possible.

5. Email Security

Emails can contain malicious content and malware. To reduce harm, the Participants should employ the following strategies:

(a) Do not open attachments or click any links where content is not well explained.

(b) Check the email addresses and names of senders.

(c) Search for inconsistencies.

(d) Block junk, spam and scam emails.

(e) Avoid emails that contain common scam subject lines such as prizes, products and money transfers.

(f) Where an email requests financial payment, confirmation of password, or prompts to login to a Company system, extreme care should be taken to ensure that it is genuine, including by calling the sender on an independently sourced contact number.

(g) Contact HILT's IT service provider when a suspicious email or other perceived cyber threat is received.

If the Participant is not sure that an email, or any type of data is safe, the Participant should contact the Chief Operating Officer at HILT CRC.

6. Device Security and Using Personal Devices

(a) Logging in to any work accounts on personal devices such as mobile phones, tablets or laptops, can put Company data at risk.

Where Company data is accessed from personal devices the Participants are obligated to keep their devices in a safe place and not exposed to anyone else.

(b) The Participants are recommended to follow these best practice steps:

(i) Keep all electronic devices' passwords secure and protected.

(ii) Logging into accounts should only be performed through safe networks.

(iii) Install security updates on a regular basis.

(iv) Upgrade antivirus software on a regular basis.

(v) Never leave devices unprotected and exposed, particularly in public spaces.

(vi) Lock computers when leaving the desk.

(vii) When accessing trusted external systems, all applicable guidelines must be complied with.

(c) It is recommended that any Internet of Things (IoT) devices are kept segregated from Company systems unless they have been approved by an IT specialist for use.

(d) The Participants must not use unauthorised devices on their workstations, unless they have received specific authorisation from the Chief Operating Officer.

(e) Any devices deemed no longer suitable for use must be disposed of in a secure way to ensure all information is permanently removed.

7. Transferring Data

Data transfer is a common cause of cybercrime. The Participants should follow these best practices when transferring data:

(a) Avoid transferring personal information such as customer data and employee information (this includes anything that can or may identify an individual including first name, last name, age, address and email address).

(b) Adhere to the relevant personal information legislation including the Australian Privacy Principles.

(c) Data should only be shared over authorised networks.

(d) If applicable, destroy any sensitive data when it is no longer needed.

(e) HILT projects contain information that is confidential. Transfer of data onto unsecure networks such as USB drives poses a particular risk and should be avoided wherever possible.

8. Working Remotely

When working remotely, all the cybersecurity policies and procedures must be followed. When travelling overseas Employees will need to seek the approval of the Chief Operating Officer and notify the Company's IT Provider should they wish take Company devices and/or access company systems.

9. Company Systems

(a) When accessing the internet from any system set up by the Company:

(i) Participants must use the standard process and not bypass any security measure.

(ii) Reasonable care must be taken in relation when downloading documents and transmitting data over the internet. Access only trusted websites.

(b) When accessing accounts on Company systems:

(i) User accounts on work systems are only to be used for the business purposes of the Company and not to be used for personal activities.

(ii) Participants are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords. Participants are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside of the Company.

(iii) Participants must not purposely engage in any activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Company systems for which they do not have authorisation.

10. General Security Requirements

(a) The Company aims to maintain a secure IT environment that is a minimum of 'Maturity Level 2' under The Australian Signals Directorate (ASD) Essential Eight Maturity Mode.

(b) In relation to the 'HILT Hub' project management system:

(i) The Chief Operating Officer of HILT CRC must approve new users
(ii) Private project groups will be established for each project where confidential information may be shared, users will be restricted to those directly involved in each project.
(iii) The Company will undertake at least annually a review of user permissions removing unnecessary access and users.
(iv) Regular password resets will be required and new users will receive a message outlining confidentiality and password protection requirements.

(c) Participants must not install unauthorised software. The Company may at any time introduce a whitelist of approved/trusted programs. If this occurs then only these programs may be used by the Participants.

(d) Participants should stay up-to-date with any other Company-wide recommendations, such as recommended browser settings.

(e) Participants must not attempt to turn off or circumvent any security measures.

(f) Participants must report any security breaches, suspicious activities or issues that may cause a cyber security breach to the Chief Operating Officer of HILT CRC immediately and await their instructions regarding the appropriate response to the breach.

(g) Participants must protect the physical security of their devices such as laptops at all times. This includes not leaving devices unattended in unsecure places where theft could occur, and locking office doors when unattended by HILT staff.

11. 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) Data Breach Policy
(b) Privacy Policy

12. Training

All Participants must maintain working knowledge of basic cybersecurity protocols. All new HILT CRC Employees will be given training on cybersecurity.

13. Disciplinary Action

If this policy is breached, one or more of the following disciplinary actions will take place:

(a) Incidents will be assessed on a case-by-case basis.

(b) In case of breaches that are intentional or repeated or cases that cause direct harm to the Company, Participants may face serious disciplinary action, including termination of your employment, engagement or services.

(c) Subject to the gravity of the breach, formal warnings may be issued to the offending Participants.

14. 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