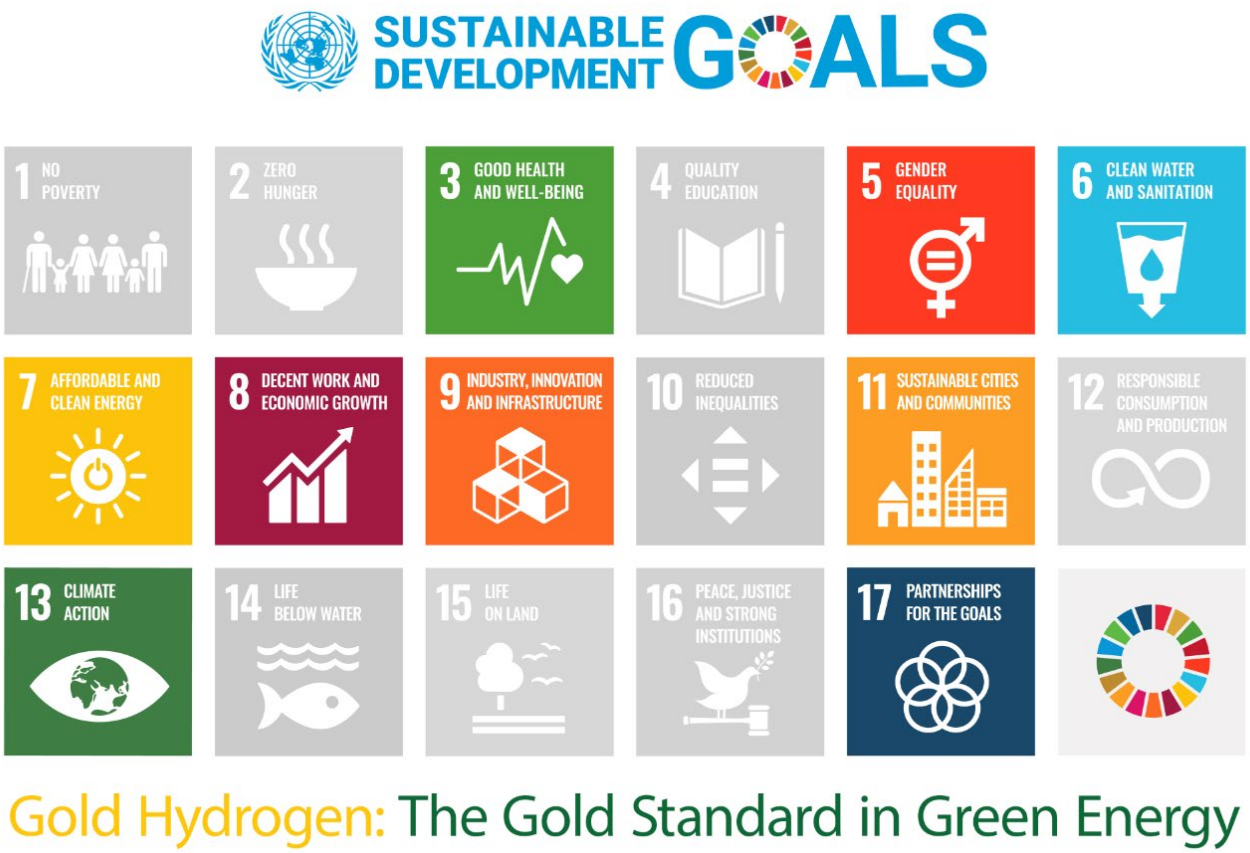
FRAUD CONTROL POLICY

GOLD HYDROGEN LIMITED

ABN 74 647 468 899



1. Purpose

Gold Hydrogen Limited (**Company** or **Gold Hydrogen**) is committed to the highest standards of conduct and ethical behaviour in all of its project and business activities, as enshrined in the Company's core values and its Code of Conduct and Business Ethics. The Company has **zero tolerance** for wilful breaches of these documents and policies, and this Fraud Control Policy.

The Company's values support a workplace culture that fosters high standards of ethical behaviour with controls in place to reduce the opportunity for fraudulent activity, making or receiving bribes or participating in corrupt behaviour.

The purpose of this Policy is to:

(a) help deter wrongdoing, in line with the Company's risk management and governance framework;

(b) support the Company's Delegation of Authority;

(c) support the Company's long-term sustainability and reputation;

(d) meet the Company's legal and regulatory obligations; and

(e) protect the investment made by the Company's shareholders.

2. Definitions and Interpretation

2.1 Definitions

In this Policy:

ARMC means the audit and risk management committee of the Board from time to time.

Board means the board of Directors of the Company from time to time.

Chief Financial Officer means the chief financial officer of the Company.

Company Secretary means a person appointed by the Company to be the company secretary.

Director means any person holding the position of a director of the Company and includes an alternate director and Directors means the directors for the time being of the Company or as the context permits such number of them as have authority to act for the Company.

Fraud Response Team comprises at least one member from the ARMC, and the Managing Director and / or CFO as appropriate.

Management means the executive management of the Company.

Policy means this Fraud Control Policy.

2.2 Interpretation

Unless the contrary intention appears, a reference in this Policy to:

(a) the singular includes the plural and vice versa;

(b) an item, recital, clause, subclause, paragraph, schedule or attachment is to an item, recital, clause, subclause, paragraph of, or schedule or attachment to, this Policy and a reference to this Policy includes any schedule or attachment; and

(c) headings are for ease of reference only and do not affect the meaning or interpretation of this Policy.

3. Introduction

3.1 Fraud

Fraud involves dishonestly obtaining an advantage through the intentional misrepresentation, deception or concealment of information. General examples of fraud potentially manifesting at the Company, whether from within the organisation itself or from an external source, include:

(a) financial theft or misappropriation of cash or securities;

(b) improper or unauthorised expenditure;

(c) unauthorised or inappropriate access to or release of information;

(d) forgery and alteration of documents;

(e) inappropriate use of insider knowledge;

(f) misappropriation or misallocation of organisational resources, such as computer or telecoms equipment;

(g) inappropriate or favourable treatment of associated parties for personal benefit;

(h) falsification of records and data, such as payment or payroll records; and

(i) fraudulent financial reporting.

3.2 Prohibition on Fraud

The Company and its Directors, executive, employees, contractors and consultants must not, directly or indirectly, authorise or participate in any form of fraud.

3.3 Fraud Control Framework

Broadly, the Company's Fraud Control Framework consists of the following elements:

(a) A **Whistlebower Policy** to provide an environment for the reporting of any incidents of fraud, with protection ensured for the whistleblower and guidelines for the conduct of investigations and reporting of incidents and outcomes;

(b) **Fraud Risk Identification** – the identification and assessment of specific fraud risks applicable to the Company, specifically including in relation to financial payment and authorisation procedures;

(c) **Fraud Mitigation -** implementation of both preventative and detective fraud control measures to reduce the risk of fraud occurrence and to allow for prompt identification of incidents if they occur, particularly as they relate to financial payment and authorisation procedures (refer to the Company's **Financial Payment & Approvals Procedures**);

(d) **Fraud Incident Response** – an annual fraud risk assessment is conducted by the ARMC to identify and document key fraud risks and associated mitigations. In addition, fraud is considered in the majority of the audits performed by the ARMC and also by external auditors; and

(e) **Reporting** - regular reporting of fraud risks and any fraud incidents is undertaken to the ARMC.

3.4 Reducing Risk

The Company notes the following factors which can be used to reduce the risk of fraud:

Cost control focus	There is a strong culture of sustainable cost control within the organisation encouraging close review of resource usage.
Strong safeguards for whistleblowing	There are strong protections (including confidentiality) afforded to those who report fraud incidents, enshrined in the Company's **Whistleblower Policy.**
Oversight	There is the necessary oversight of the transactions and activities of the Company and its subsidiaries that are susceptible to fraud incidents. Refer to the Company's documented **Financial Payment & Approvals Procedures.**
Tone from the top	Management and the Board set an appropriate fraud control "tone from the top".

4. Objectives and Principles

4.1 Objectives

The objectives of this Fraud Control Framework are to:

(a) identify and assess potential risks and sources of fraud within the organisation;

(b) design effective mitigating controls to reduce the opportunity to commit fraud and detect its occurrence should the preventative controls not be designed or operating effectively;

(c) enable effective responses and investigations into fraud incidents to reduce their impact and potential loss amounts;

(d) provide a mechanism and environment for staff to report suspected fraud incidents; and

(e) facilitate reporting of the fraud control environment and timely reporting of fraud incidents.

4.2 Principles

The key principles governing this Fraud Control Framework and application are:

(a) a zero tolerance approach to fraudulent or dishonest activity within, or in connection with, the Company, its subsidiaries and its projects and activities;

(b) responses to fraud incidents need to be objective, timely and comprehensive; and

(c) staff are required to contribute to the minimisation of fraud occurrence and impacts.

5. Scope

The Company's fraud control framework applies to any activities potentially subject to fraud, or suspected fraud, involving employees, consultants, vendors or contractors and/ or any other parties with a corporate relationship with the Company in connection with any of its subsidiaries, projects or activities. This includes fraud associated with cyber security risks such as phishing and malware (ransomware) intrusion.

6. Roles and Responsibilities

6.1 ARMC

The ARMC has reviewed and endorsed this Fraud Control Policy and is responsible for receiving reports of fraud incidents, and tracking and monitoring agreed actions to address the impacts of fraud.

6.2 Fraud Response Team

At least one member of the ARMC, together with the Company's MD and / or CFO are to form a Fraud Response Team in the event a significant fraud is suspected, or an investigation initiated. Where appropriate, the Company's Board Chair may also be involved. The team shall have recourse and authority to engage with external experts as required (lawyers, forensic accountants, etc).

6.3 Management and the Board

The Company's Board and management are required to set the ethical 'tone from the top' to flow throughout the Company to entrench a culture of high ethics and integrity.

6.4 Gold Hydrogen Staff

The Company's staff, contractors and consultants are required to:

(a) perform their roles and tasks ethically and diligently;

(b) be vigilant and report any instances of suspected fraud promptly; and

(c) actively participate in any Company initiated fraud awareness training, as required.

7. Fraud Identification, Prevention and Response Procedures

As outlined in detail in Schedule 1 and Schedule 2 to this Policy.

8. Reporting

8.1 Fraud Incident Reporting

Noting legal and other considerations, fraud related incidents and outcomes of fraud investigations are to be reported to the ARMC and external parties as appropriate.

The Board will be informed of any breaches of this Policy.

8.2 **External Audit**

External Audits are required to perform certain fraud procedures and report to the ARMC if they have observed any indications of fraud during their audit enquiries and procedures.

9. Relationship to Other Policies and Documents

This policy should be considered with reference to the following underlying policies and documents published by the Company:

(a) Statement of Core Values;

(b) Code of Conduct and Business Ethics;

(c) Anti-Bribery and Corruption Policy;

(d) Financial Payment Authorisation Procedures; and

(e) Whistleblower Policy.

Version	Last periodic review	Last update	Approver
1.0	August 2022	August 2022	Board

Schedule 1 – Fraud Identification, Prevention and Incident Response Procedures

1 Identification and Analysis

The Company's Board and management are to assess existing and new business activities for fraud risks. As with other risk categories, identified fraud risks are to be assessed in terms of likelihood of occurrence and impact to the organisation.

2 Mitigating Fraud Controls

Control procedures to mitigate the risk of fraud can either be preventative or detective, or both, in nature. Examples of each include:

Preventative

- workplace policies and culture promoting and encouraging ethical behaviour including fraud awareness training;
- pre-employment screening and background checks where new employees and contractors acknowledgement of policies upon commencement;
- regular policy updates and communication to staff;
- high risk employees subject to annual acknowledgement of some policies;
- authorisation and dual check controls within key processes, including segregation of duties;
- periodic review of fraud risks and scenarios;
- system access controls;
- centralised operations;
- automated daily transaction processing; and
- physical security controls,

Detective

- escalation and provision of whistleblowing through letter, internal mail or anonymous mail;
- reviews of exception reports and reconciliations and other management reporting;
- exception reporting for some systems;
- periods of consecutive staff leave without office/telecommunication contact; and
- assurance and compliance functions.

These controls are either purposely implemented to prevent fraud or by their nature indirectly reduce the risk of fraud.

(1) Primary Fraud Controls

These are controls which are specifically designed to reduce the risk of fraud occurring and usually operate 'nearby' to physical assets. Segregation of duties between specific functions, the requirement for dual transaction authorising signatories and input/checker transaction approval procedures are examples of primary fraud controls.

The Company has a documented framework dealing with its Financial Payment & Approvals Procedures which should be read by staff, contractors and consultants in conjunction with this policy.

(2) Secondary Fraud Controls

These are controls which have primary objectives of accuracy, validity and completeness, but their presence acts to deter or detect fraud. Examples include bank and system reconciliations, and supervisory reviews.

(3) Risk culture

Risk culture manifests itself in the risk attitudes ethics, integrity and competence of the people within an organisation. It is influenced by management's operating style and philosophy, the way management assigns responsibility and authority, the way the organisation structures and develops its people and the attention and direction provided by the Board. The key elements of the Company's risk culture contributing to an effective fraud control environment include:

- Board and management-defined policies and procedures (including the Company's Corporate Code of Conduct and Business Ethics, Anti-Bribery and Corruption Policy, Whistleblower Policy, Audit and Risk Management Committee Charter, People, Culture and Resources Committee Charter, Nomination Committee Charter, Diversity Policy, and the ESG Committee Charter);
- a culture of recognition and compliance with the organisational responsibilities in regard to regulatory, environmental and social issues;
- performance, remuneration and reward strategies and commitment to promote competence, compliance and development of staff;
- an independent Board and requisite oversight committees;
- an organisational structure that promotes independent internal audit, risk management and compliance functions; and
- management focus on operational issues and willingness to discuss and address potential control weaknesses.

(4) Fraud Awareness

A common way in which internal fraud is detected is by observation and reporting by workplace colleagues of the perpetrator(s). Similarly, a likely way for externally instigated fraud to be detected is by an employee of the victim organisation. It is therefore important that Company staff have a general awareness of fraud and the appropriate response to be adopted if this type of activity is detected or suspected.

The Company's MD or CFO in conjunction is to co-ordinate organisation-wide fraud control training as required (recommended on at least a two yearly basis).

3 Fraud Incident Response

Detection and Escalation

A key aim of the fraud control framework is the early detection and escalation of fraud incidents within the organisation. A culture of fraud awareness and openness in relation to fraud reporting should be encouraged with escalation to the Company's MD, ARMC and / or Board as appropriate. Any party reporting the alleged fraud may be afforded protection as outlined in the Company's Whistleblower Policy.

Investigation

Upon notification of a fraud event, the Fraud Response Team are to:

- identify and assess required team members;
- determine requirements to notify law enforcement or regulatory agencies of events;
- determine whether to seek to recover any misappropriated monies or assets;
- make recommendations regarding sanctions on the employees involved, up to and including terminations;
- notify insurers of fraud as required;
- implement appropriate stakeholder interaction procedures, covering media, investors, regulators, etc;
- define and conduct investigation procedures;
- engage external specialists as required; and
- assess investigation results and propose recommended actions.

Remediation

Agreed actions to address the impacts of the fraud should be tracked and monitored by the ARMC.

Disciplinary Action

Committing a fraudulent act and breach of internal policy is viewed seriously by the Company, and staff found to be involved will be subject to disciplinary action. Staff are required to escalate any indications or occurrences of fraud.

4 Fraud Assessment

ARMC

The ARMC conducts two types of fraud review and assessment activities:

- high level, annual assessment of fraud risks across the Company; and
- detailed assessment of fraud risks as part of each audit review conducted.

The ARMC is to include fraud risk in their audit scopes and undertake an annual fraud risk assessment.

Schedule 2 – Fraud Response Checklist

The following table includes guidance for the Fraud Response Team on areas to be considered in the event of a suspected fraud event.

Area	Action	Considerations	Responsibility	Status
Fraud Response Team Composition	Agree composition of Fraud Response Team	• Chair • Independence / Objectivity / Conflicts of interest • Size and nature of fraud • Required skills sets • Establishment of specific investigation team	ARMC, CEO, CFO	
Police Notification	Determine requirements to notify law enforcement agencies of events	• State Police Fraud Squad	CEO, CFO	
Asset Recovery	Make recommendation to seek to recover any missing money or assets	• Speedy recovery response action more likely to be successful	Fraud Response Team	
Staff	Make recommenda-tions regarding appropriate remediation/dis-ciplinary actions.	• Employment laws • Suspensions	CEO, CFO	
Confidentiality	Remind and enforce confidentiality requirements around the Fraud Response Team activities	• Confidential treatment of response actions is important in the management of potential negative impacts of fraud. • Internal and external parties	Fraud Response Team	

Area	Action	Considerations	Responsibility	Status
Evidence	Implement arrangements to secure evidence	Potential to seek legal remedy influenced by sufficiency of evidence. • Interviews • Telephone records • Data recovery • External parties.	CEO, CFO	
Insurance	Notify insurers of fraud as required.	• Bond, Electronic & Computer Crime Policy • Fidelity policy	CEO, CFO	
Stakeholders	Implement appropriate stakeholder interaction procedures, covering media, investors, regulators, etc.	• Media • Investors • Regulators • Staff	Fraud Response Team	
Investigation	Define and conduct investigation procedures	• Scope • Procedures • Event facts • Accountabilities • Root causes	ARMC	
Recommendations	Assess investigation results and propose recommended actions.	• Present results to the Board	ARMC	