Fraud Policy

SG-LSC-GP-2A3

Version 3.1

9 December 2021

1. Background and Purpose

Good corporate governance requires that appropriate mechanisms be in place for fraud risk management, including policies and procedures, risk assessment, internal controls, investigation, reporting and education to reduce the incidence of fraud.

The Board has established this Fraud Policy to:

- give effect to, and provide clarity on, Sigma's commitment to prevent and control fraud and corruption;
- support the development and maintenance of a sound ethical culture across Sigma, recognising that raising awareness of ethical behaviours amongst team members assists in minimising the risk of fraud across the business; and
- articulate roles and responsibilities across the organisation for assisting in the detection, prevention, monitoring, reporting and investigation of fraud.

The Board and Management recognise that good fraud governance requires more than just ensuring an effective system of internal controls. It requires all team members to work together to lead by example, with knowledge of the key fraud risks, to sponsor awareness, encourage effective reporting and champion a strong culture of ethics and honesty.

2. Application

This Fraud Policy applies to all activities potentially subject to fraud, involving team members; consultants; suppliers; contractors and any other parties with a corporate relationship with any Sigma company in any location.

Sigma publishes a copy of this Fraud Policy on Sigma's intranet.

3. Main points for team members

Company Position on Fraud	Expected Behaviours of Sigma team members	Internal Controls and processes
• Sigma does not tolerate fraudulent conduct by its team members or others that do business with Sigma. • Suspected fraudulent conduct should be reported and is taken seriously and investigated. • Action is taken against those who are found to have acted fraudulently including, where appropriate, disciplinary action, referral for criminal prosecution; and/or civil action to recover funds and related losses.	• All team members are expected to play a role assisting in the prevention, detection and reporting of suspected fraudulent conduct. • All team members are expected to be guided by Sigma's Code of Conduct, compliance standards and supporting policies in day to day decision-making. • Concerns should be raised through appropriate reporting channels. • Team members are expected to participate in training, awareness raising, monitoring and review activities.	• The policy aligns with, and should be read in conjunction with, Sigma's Code of Conduct, Whistleblower Policy and Risk Management Framework.

4. What is fraud or corruption?

Definition and general examples at Sigma

Fraud involves dishonestly obtaining an advantage through the intentional misrepresentation, deception, or concealment of information. Fraud includes activities such as deception, bribery, forgery, extortion, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts or other activities that involve an act of deceit against Sigma to obtain a personal or collective advantage, avoid an obligation or cause a loss. It is not restricted to monetary or material gain. Fraud and corruption may include intangible benefits such as status or information.

General examples of fraud that could potentially occur at Sigma, whether from within the organisation itself or from an external source, include:

	Examples
	financial theft or misappropriation of cash (e.g. payment to phantom employees, payment to employees or contractors for tasks not performed)
	theft of medicines or other products that Sigma distributes (e.g. sale of Sigma products for personal gain or theft for own use)
	improper or unauthorised expenditure including on company credit cards (e.g. luxurious or excessive expenditure, inflated or faked expense claims, personal expenditure)
	unauthorised or inappropriate access to, or release of, data or information (including hacking or any activity that compromises cyber security)
	forgery or alteration of documents and withholding documents (e.g. misrepresentation of qualifications to obtain employment, providing false or misleading information or not providing information when there is a legal obligation to do so)
	inappropriate use of insider knowledge and information (e.g. disclosing Sigma's confidential information for personal gain without authority, or dealing, or getting others to deal, in Sigma securities while in possession of unpublished price-sensitive information)
	misappropriation or misallocation of Sigma's resources, such as computer or technology equipment or other company supplies
	inappropriate or favourable treatment of: suppliers; contractors; team members or potential team members; customers; consultants or other people that Sigma does business with for personal benefit. For example, awarding contracts to suppliers for personal gain or hiring/promoting inappropriately.
	falsification of records and data, such as payments or payroll records or hours worked (eg clocking in early)
	fraudulent financial reporting (e.g. misrepresenting financial statements, or misstating or omitting financial accounting information, to give investors a mistaken impression about Sigma's operating performance and profitability)
	IP theft including leaking trade secrets, confidential information or patents to competitors (note these obligations continue beyond the term of your employment at Sigma)
	Identity theft through misuse of personal or sensitive information.
	Getting injured outside of work and claiming the injury occurred at work or falsifying an illness or injury to inappropriately receive workers compensation.

Factors identified that could increase the risk of fraud at Sigma include:

- fast moving business across multiple sites
- processing of high value, high volume transactions
- complex and variant systems across the organisation that could make it difficult to control system security access
- multiple site / split site team operations and organisation restructures
- ongoing business acquisitions / expansion and an increasing number of initiatives

- sales based reward programs
- some key procedures and controls are performed manually
- concentrated business and system knowledge
- potential for collusion on the part of employees, customers or suppliers
- unrestricted access to information

5. What is not fraud?

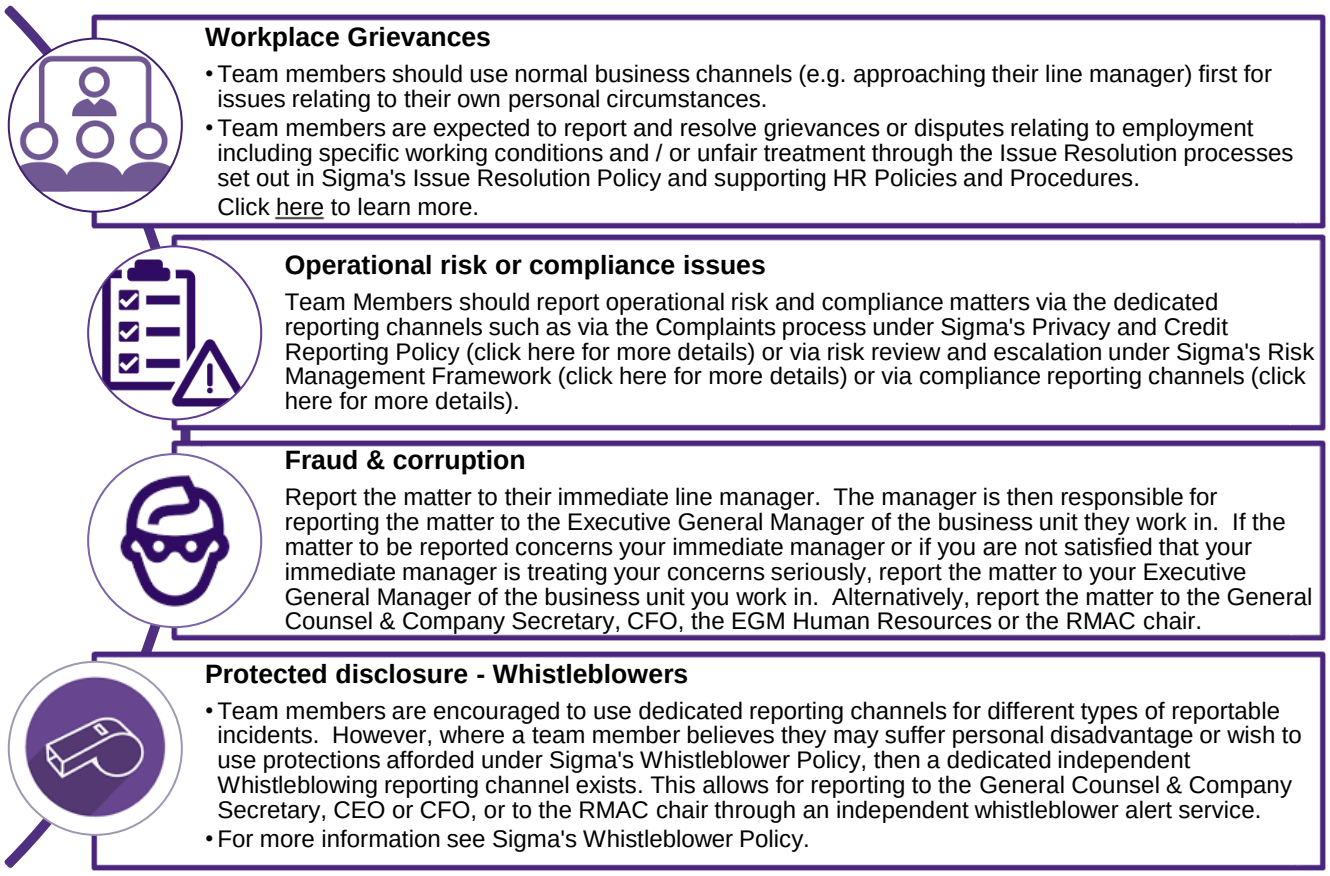
Other breaches of Code of Conduct

Engagement in fraudulent activity or corruption is a breach of Sigma's Code of Conduct. However, not all Code of Conduct breaches are fraudulent or corrupt. Examples of breaches of Sigma's Code of Conduct which are not fraud or corruption include:

- workplace grievances, such as complaints of injustice in the assessment of a team member's performance or disciplinary procedures;
- complaints of discrimination, harassment or bullying;
- reports of suspected breaches of Sigma's Health and Safety Policy; and
- reports of suspected breaches of other laws and regulations which apply to Sigma's operations.

Reporting channels

Across Sigma there are several policies and codes which each promote a culture of conducting our business with honesty, fairness and integrity. There are dedicated reporting channels which exist under those policies and codes. The key reporting channels are summarised below.



6. General obligations of all team members

✗	Engage in, participate in, cover up or in any way assist in (including by failing to act) any form of fraud or corrupt conduct.
✗	Engage in, participate in, cover up or in any way assist in (including by failing to act) any behaviour or conduct which involves or may be perceived as victimisation, bullying, harassment or any other form of reprisal action against: • another team member who makes a report of wrongdoing covered by this Policy; or • any person against whom allegations of wrongdoing have been made if the results of the internal inquiry or investigation show they were not implicated in improper behaviour.
✓	Comply with the internal controls, systems, relevant policies and directions as apply to team members in relation to carrying out duties or functions. Examples of these internal controls include policies and procedures, financial delegation and approval authority. (The objectives of such internal controls include assisting in the prevention, deterrence and detection of the type of conduct prohibited by this Policy.)
✓	Take steps to protect company and personal information including restrict access to certain documents and files.
✓	Be alert and wary of various and emerging types of fraudulent activity eg ‘payment redirection fraud’ where a fraudster impersonates someone such as the CEO by email and directs team members to pay to a different account.
✓	Familiarise yourselves with this Policy and with related policies such as the Code of Conduct, Whistleblower Policy, Anti-Bribery & Corruption and Delegations of Authority.
✓	Report any incident you become aware of involving (or which you reasonably believe involves) fraud or corrupt conduct.
✓	Report any conduct that you reasonably believe constitutes detrimental or reprisal action against a person who has made a report of wrongdoing under this Policy.

7. Additional responsibilities of Management

To ensure that Sigma conducts itself and carries out its duties and activities free from fraud and corrupt conduct, Managers and Supervisors must ensure compliance with the following obligations and responsibilities in addition to the general obligations outlined above.

✓	Be familiar with the types of misconduct that might occur within your area of responsibility and be attentive to any sign of wrongdoing.
✓	Ensure that those reporting to you comply with the internal controls, systems, relevant polices and directions as apply to them in relation to carrying out their duties or functions.
✓	Treat seriously all reports of alleged fraud and corrupt conduct and ensure that such reports are dealt with in accordance with the applicable procedures.
✓	Take such action as is required to prevent retaliation or retribution against a person who has made a report of fraud or corrupt conduct.
✓	Promote awareness of this Policy and related policies to all team members reporting to you.

8. Additional responsibilities of team members with Financial Delegations

Any person with financial delegation or responsibility for administering financial transactions is required to comply with their assigned delegation and comply with all relevant finance policies and procedures, financial systems requirements and other financial controls of Sigma.

9. Expectation

All team members are expected to report known, suspected or potential cases of conduct which is in breach of Sigma's Code of Conduct through the appropriate reporting channels to enable Sigma to consider any appropriate action.

Confidential treatment of reporting actions, information provided by team members and response actions is important. Individual confidentiality will be respected throughout the reporting and investigation process. Reporting team members may remain anonymous to the extent possible by law (refer to the Whistleblower Policy).

10. Fraud Investigation

The process for fraud investigation will depend on the severity and complexity of the suspected fraud event. The investigation team may comprise:

- General Counsel;
- EGM Human Resources;
- Chief Financial Officer;
- Members of Internal Audit; and
- External consultants and specialists.

Actions

The investigation team will:

- define and conduct investigations;
- engage external specialists as required;
- assess investigation results and propose recommended actions;
- consider whether to notify law enforcement or regulatory agencies of events (engage with RMAC Chair where appropriate);
- 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; and
- implement appropriate stakeholder interaction procedures, covering media, investors, regulators, etc.

A checklist for the typical investigation process is attached to the Policy – Attachment 1.

Investigation process

The investigation team formed to investigate the report will be required to follow normal Sigma procedures for handling a complaint or disciplinary issue. This would generally involve:

- undertaking a fair, independent and discreet investigation into the substance of the report to determine whether there is evidence to support the matters raised;
- respecting individual confidentiality;
- collecting all available data and verifying the reported information; and
- proceeding with due care and appropriate speed.

Disciplinary Action

Committing a fraudulent act and breach of internal policy is viewed seriously by Sigma and team members found to be involved will be subject to disciplinary action. Disciplinary action may include termination of employment, recovery of losses / proceeds (including by way of civil action) and/or reporting to Police for criminal prosecution.

Remediation

Agreed actions to address the impacts of the fraud will be tracked and monitored by the investigation team.

11. Reporting to RMAC

Fraud related incidents and suspected fraud incidents are to be reported to the CEO and RMAC chair. Progress of and outcomes of fraud investigations are to be reported to the RMAC and external parties as appropriate.

Related internal policy breaches (if any) must follow the applicable reporting procedure set out in the relevant policy. Should Internal Audit or External Audit activities detect any instance of fraud, these will be reported to RMAC.

12. Interpretation

In this policy, unless the context otherwise requires:

- the singular includes the plural and vice versa;
- another grammatical form of a defined word or expression has, when capitalised or otherwise used, a corresponding meaning;
- a reference to a person (or someone else) includes an individual, body corporate, partnership, firm, association or other entity;
- the meaning of general words is not limited by specific examples introduced by including, for example or similar expressions; and
- a reference to a section or a schedule is to a section or schedule of this policy.

Headings are for convenience only and do not affect interpretation.

13. Defined terms

In this policy (unless the context otherwise requires):

Term	Definition
Board	means the Directors of Sigma from time to time, acting as a board.
Company Secretary	Means the company secretary of Sigma
Executive Team	Means any team member reporting to the CEO who is disclosed as a member of the executive team
External Audit	Sigma's appointed external auditors
Internal Audit	Means Sigma's appointed internal auditors
RMAC	Means the Board's Risk Management and Audit Committee
Sigma Group	Means Sigma and its subsidiaries
Sigma	Means Sigma Healthcare Limited ABN 15 088 417 403
Team Member	means any full time, part time or casual employee of any member of Sigma Group and extends to any secondee, contractor or consultant of, or adviser to, any member of Sigma Group whose terms of engagement require them to comply with this policy as though they were an employee.

14. Further information

Monitoring compliance

Sigma may audit compliance with this policy by any team member (or other person subject to this policy).

More information

If you have any questions arising from this policy, please contact the Company Secretary.

15. Document control and related documents

Name of Document	Fraud Policy		SG-LSC-GP-2A3
Document Author	General Counsel		
Document Approver	Board		Dec 2021 Board Meeting
Document Reviewers	CFO		RMAC
Review Period	Two-yearly		
Related Documents	Code of Conduct, Whistleblower Policy		
Change Record	Version	2.0	Change Notes
	Publish Date	9 December 2021	Minor, non-substantive amendments Fraud Policy v2.1 published 9 December 2020 and Board feedback on 9 December 2021

Attachment 1 – Fraud Investigation Checklist

Area	Action	Responsibility	Status
Investigation Team Composition	Agree composition of Investigation Team	CPO in consultation with CFO and General Counsel & Company Secretary	
Police notification	Consider whether notification is required to law enforcement agencies of the event and other regulatory bodies as appropriate. Engage with RMAC Chair where required.	General Counsel & Company Secretary in consultation with CPO and CFO	
Asset recovery	Make recommendations to seek to recover assets / funds	CPO in consultation with CFO and General Counsel & Company Secretary	
Team Members	Make recommendations regarding appropriate remediation / disciplinary actions	CPO in consultation with CFO and General Counsel & Company Secretary	
Confidentiality	Remind and enforce confidentiality requirements around Investigation Team activities	General Counsel & Company Secretary in consultation with CPO and CFO	
Evidence	Implement arrangements to gather and secure evidence gathered	General Counsel & Company Secretary in consultation with CPO and CFO	
Insurance	Notify insurers as required	General Counsel & Company Secretary in consultation with CPO and CFO	
Investigation	Define and conduct investigation appropriate to complexity and area of suspected fraud	CPO in consultation with CFO and General Counsel & Company Secretary	
Recommendations	Assess investigation results and propose recommendations	Investigation Team	