CSL Group Anti-fraud Policy

Purpose and Scope

CSL applies a "zero tolerance" approach to acts of fraud by any of our employees, officials, representatives, or third-party contractors; hereafter referred to as "CSL Persons".

CSL has a well-established reputation for conducting business in an ethical and honest way. This reputation is built on our company value of Integrity, which is a major, underlying theme throughout our Code of Conduct.

CSL is committed to acting with integrity and protecting our reputation, assets, and stakeholders against the potential risk of fraud. CSL recognises that any instance of fraud can have a significant negative impact on our image and reputation xand on the opinion our patients, donors, customers, employees, global communities, shareholders and other stakeholders hold of us.

Management (which in this policy includes all functional and business, global and local managers) has the primary responsibility for implementing this policy within their areas of responsibility.

Any breach of this Policy will be regarded as a serious matter and will result in disciplinary action up to and including termination of employment or termination of a contractual relation with any third party.

The policy applies to CSL Limited and is to be implemented across all CSL Group Companies. CSL refers to CSL Limited and all CSL Group companies.

1. What is Fraud

Fraud, whether committed internally (by employees, contractors or business partners) or externally (by customers, vendors, or third parties), is a deliberate act involving the use of deception or dishonesty to obtain an unfair, unauthorised or illegal advantage, whether financial or otherwise, for their benefit or the benefit of others.

Fraud may include falsification, concealment, misrepresentation or unauthorised destruction of documentation, data or information used or intended for use for CSL business purposes. Fraud also includes the misuse of confidential information or company resources for personal or third-party benefit.

Examples of Fraud include, but are not limited to:

- Misappropriation or unauthorised use of company's funds, property, supplies or other assets including use of assets for private purposes;
- Unauthorised use of CSL's legal identity or business name and/or ACN (Australian Company Number), ABN (Australian Business Number) or identification details for the illegal transactions, including import and/or export of items;
- Causing a loss to CSL or creating a liability for CSL by dishonesty or deception;
- Manipulation or misstatement of financial or business reports, records, or internal controls, including expense claims, timesheets or financial disclosures;
- Unauthorised access or misuse of confidential or proprietary information, including insider knowledge of CSL activities for personal or third-party benefit, including leaking sensitive company data;
- False invoicing for goods or services not received or rendered;
- Submission of exaggerated or fictitious accident, harassment or injury claims;
- Misuse or falsification of leave;
- Use of CSL's systems or technology to facilitate fraudulent activities, including altering digital records, sending scam emails from a company email or exfiltrating sensitive data via private, non CSL authorised, cloud services; or
- Collusion with third-parties to commit any of the above acts.

2. Who May be Guilty of Fraud

Fraud may be committed by any:

- CSL employee, officer, or director; or
- Person acting on behalf of another i.e., a Third-party individual or organisation acting on behalf of CSL or representing CSL in a market (i.e. a third-party contractor or representative, distributor or agent); or
- Any person or organisation which authorises, permits or facilitates others to carry out such acts.

Fraud is a criminal offence, and penalties can be severe for both companies and individuals. There is legislation in every country that prohibits Fraud and is enforced with vigour by enforcement authorities.

3. Fraud Prevention

A. Risk Assessment

Managers must assess the vulnerability of their business or functional area of responsibility to fraud risk. Where fraud risks are identified, they should be managed in accordance with CSL's established Enterprise Risk Management Framework (ERMF).

B. Accurate Record-Keeping

Managers must ensure that all business records and overall financial reporting within their scope of control is transparent and fully compliant. They must accurately reflect each and all underlying transactions. Managers are responsible for performing a diligent oversight of any business records and financial transactions to prevent instances of fraud.

C. Effective Monitoring and Control

Managers must take the necessary steps to maintain an effective system of internal controls and monitoring to prevent fraud. This must include ensuring CSL Persons are aware of and understand this Policy through education and training.

Managers must provide a sign off which ultimately is provided to the CSL Chief Financial Officer (CFO) and Chief Executive Officer (CEO) as part of the annual management representation process that the business or functional area that they are responsible for has assessed the vulnerability of its operations to Fraud risks, and that appropriate controls and monitoring have been put in place to prevent Fraud and to the best of their knowledge, that there have been no instances of Fraud that have not otherwise been reported to Senior Management or through the channels outlined in this Policy.

4. How to Raise a Concern

All CSL Persons have a responsibility to help detect, prevent and report instances not only of Fraud, but also of any other suspicious activity or wrongdoing in connection with CSL's business. CSL is committed to ensuring that all CSL Persons have a safe, reliable, and confidential way of reporting any suspicious activity.

CSL Persons should report the issue/concern directly to the CSL Ethics & Compliance team in the first instance, via telephone, email, or in person, or to a named member of the Fraud Evaluation Committee (FEC) as noted in this policy. If they feel comfortable to do so, this should be done with a copy to their manager or another manager.

If CSL Persons do not feel comfortable advising a manager or would prefer their report to be anonymous and/or confidential, concerns can also be reported via CSL's Speak Up Hotline. Guidance for reporting via CSL's Speak Up Hotline for CSL Persons can be found in the *CSL Group Speak up Policy.*

Reports of suspected "phishing" attempts, or suspicious email communications, received by employees should be escalated solely through the "report phishing" option in the CSL email applications. These communications will be reviewed by CSL I&T in accordance with established information security procedures and will be escalated to the FEC if it is determined that the matter represents an ongoing or potential fraud threat.

In the event that an incident of Fraud or wrongdoing is reported, CSL will act as soon as possible to evaluate the situation. CSL has clearly defined procedures for investigating fraud as well as anti-bribery and corruption, misconduct and non-compliance issues and these will be followed in any investigation of this kind. This includes keeping all investigations and reporting confidential and on a 'needs to know' basis only. In addition to any internal procedures, this includes the referral to appropriate government enforcement agencies. Any questions about these procedures should be directed to the CSL Ethics & Compliance team.

Responsibility

Employee Category	Responsibility
All employees	All CSL Persons have a responsibility to help detect, prevent, and report instances of fraud. This includes complying with CSL's policies (including the *Code of Conduct* and this Policy) and procedures and for being alert to any behaviour or actions that are inconsistent with CSL's policies and procedures and reporting suspected or attempted instances of fraud. This also includes any other instances of suspicious activity or wrongdoing in connection with CSL's business. No employee should attempt to undertake any fraud investigation, unless authorised to do so in accordance with this Policy.
Managers	Monitoring and supervising CSL Persons' conduct to deter potentially fraudulent practices; Raising awareness in relation to prevention and detection of fraud; Receiving and escalating (only if received directly by managers), reports of potential fraud and misconduct from their direct reports; Fostering an environment within their function/business area of responsibility that makes active fraud control a responsibility of all CSL Persons; Articulating and reinforcing clear standards and procedures to deter fraud, including appropriate education and training of employees; Implementing any directions in relation to the prevention and detection of fraud; Reporting all known instances of suspected or attempted Fraud to the Fraud Evaluation Committee (FEC).
Fraud Evaluation Committee (FEC)	The FEC consists of CSL's Chief Risk Officer (CRO) and Chair of the Committee, Chief Ethics & Compliance Officer (CECO), Chief Information Security Officer (CISO), Enterprise Security Head (ESH), and applicable senior leadership designees from Finance, Legal and Human Resources. The FEC is responsible for decision making, oversight, and execution for investigative matters related to fraud under this policy.

Policy Governance Details

Policy approval and review

This Policy has been approved by the Board and will be reviewed periodically by the Board or a Committee of the Board (within at least 3 years from date effective) to check that it is operating effectively and whether any changes are required.

Interpretation

The Group General Counsel will be the final arbiter for interpretation and/or clarification of this Policy. Any questions regarding the applicability of this Policy to any particular activity or omissions, should be directed to the Ethics & Compliance team or a named member of the FEC as noted in this policy.

Local Conditions

This Policy must be read in conjunction with, and is subject to, the laws and regulations in the respective jurisdictions in which CSL operates. If any local laws or regulations conflict with this Policy, or have stricter requirements, those local laws or regulations take precedence.

Training/Awareness

Training will be assigned globally to all employees of CSL irrespective of their position, level or responsibility, on commencing employment and after that, on a frequent basis. Managers are responsible for ensuring that all CSL Persons are aware of the importance and mandatory nature of this policy and that all CSL Persons have been trained and achieve a level of acceptable competence.

References

CSL Code of Conduct
CSL Group Anti-Bribery and Anti-Corruption Policy
CSL Group Speak-Up Policy