

Fraud, Bribery and Corruption Prevention Policy

1. Purpose

Stockland is committed to conducting our business ethically, with integrity and with consideration to our stakeholder expectations. Stockland does not tolerate or support corrupt or fraudulent activity of any kind. Fraud, bribery and corruption damage Stockland's reputation, can undermine political and social stability, security and human rights. It can also carry legal and criminal consequences both for Stockland and for individuals involved.

The purpose of this Policy is to set out Stockland's approach to fraud, bribery and corruption, and relevant employee guidance and obligations.

2. Scope

This Policy applies to Stockland Corporation Limited, Stockland Trust and their related companies and trusts (collectively "**Stockland**") and all Stockland employees (including but not limited to non-executive directors, permanent, casual and fixed term employees and temporary workers) ("**Employees**"). Adherence to this Policy is mandatory.

3. What is Fraud?

Fraud is dishonest activity causing actual or potential financial loss to any person or entity including theft, and where deception is used at the time, or immediately before or after the activity (defined by AS 8001-2008 – Fraud & Corruption Control). It includes destruction, concealment and falsification of documents and the improper use of information or position for personal financial gain. Fraud can be committed by an Employee or persons external to Stockland.

Examples of fraud may include, but are not limited to:

- Diversion of cash (accounts payable and receivable schemes)
- Falsifying expense claims or false invoicing
- Dishonest or deliberately misleading financial performance reporting
- Theft, unauthorised use or misuse of assets (e.g. cash, equipment, supplies) secret commissions, records and confidential information
- Unauthorised use of a credit card
- Any computer related activity involving the alteration, destruction, forgery or manipulation of data.

If Employees have any doubts about whether an activity, decision or action constitutes fraud or is otherwise inappropriate, they should seek guidance from Stockland's Group Risk team via

compliance@stockland.com.au or the Group Risk Officer. Anonymous disclosures can be raised utilising one of the reporting channels specified in Stockland's Whistleblower Policy.

4. What is Bribery and Corruption?

Corruption is a dishonest activity in which a person acts contrary to the interests of the entity they represent and abuses his or her position of trust for direct or indirect personal gain or advantage. Bribery may also be a form of corruption.

Corruption also includes dishonest activity by Stockland, or a person acting on behalf of and in the interests of Stockland, in order to secure some form of improper advantage for Stockland either directly or indirectly.

Bribery means dishonestly providing, or offering to provide, directly or indirectly, any benefit to a person with the intent of influencing the person in relation to their business, duty or affairs and/or encouraging the misuse of their authority. This includes but is not limited to foreign and domestic public officials.

Bribery can take many forms including but not limited to:

- giving cash, or lavish gifts, sponsorship, or travel and accommodation
- giving political donations which are intended to gain a specific business advantage
- paying disguised agents fees (secret commissions)
- making inflated tenders or false invoices

False accounting

It is a criminal offence to intentionally or recklessly falsify any accounting document in order to conceal or disguise the giving or receiving of an amount or benefit that is not legitimately due.

Facilitation payments

Facilitation payments, also referred to as "kickbacks" or "expedition fees", are payments of a minor value made to domestic or foreign public or government officials, to expedite or secure the performance of a routine government action by a government agency. These payments can be made either directly or by third parties. In Australia, facilitation payments may in some cases serve as a defence to the offence of bribery of a foreign public official. Notwithstanding this, Stockland does not tolerate facilitation payments or gifts of any kind to public or government officials, no matter what level of government.

5. Fraud, Bribery and Corruption Prevention Framework

Stockland is committed to a zero tolerance approach to contraventions of anti-bribery and corruption laws. The most effective means of preventing fraud, bribery and corruption is for management to foster and encourage a strong ethical culture at Stockland, and to implement policies, procedures, training, periodic audits, segregation of duties and other control mechanisms which minimise the likelihood of fraud and corruption occurring. Stockland's Fraud, Bribery and Corruption Prevention Framework interacts closely with the following Stockland Policies:

- [Risk Management Policy](#) which outlines Stockland's approach to risk management stating Stockland recognises the importance of building and fostering a risk aware culture, such that every individual takes responsibility for risks and controls in their area of authority.

- [Compliance Framework](#) which sets out the framework for managing Compliance throughout the organisation and states that Compliance with all applicable laws, regulations, industry requirements, contracts, company policies, codes of conduct, and corporate governance expectations is critical to our business success.
- The [Stockland Code of Conduct](#) sets out the standards of expected behaviour for all employees, directors, contractors and consultants in the performance of their duties.
- [Whistleblower Policy](#) which enables protected disclosures to be reported and investigated where there are reasonable grounds to suspect concerns of misconduct or an improper state of affairs within Stockland. Disclosures can be made through any of the channels specified in the Policy which include internal and external reporting and the ability to make an anonymous disclosure.
- The [Government Relations Policy](#) prohibits political donations, facilitation payments or gifts of any kind to public or government officials.
- The [Securities Trading Policy](#) and [Restricted Securities Trading Policy](#) prohibits the disclosure of inside information and sets out the permitted trading window and if other approvals are required before trading in Stockland securities.
- The [Conflicts of Interests Policy](#) outlines what is a conflict of interest, how to identify, report, assess, manage and monitor conflicts of interest that may arise within our business. The policy stipulates dollar thresholds and pre-approval required for gifts and hospitality exceeding reasonable value.
- Various accounting and expense policies that govern financial records including expense claims, accounting treatments, and anti-money laundering.
- The [IT Policy](#), [Third Party Security Policy](#) and [Information Security Policy](#) detail electronic monitoring and surveillance, importance of systems security, and responsible usage of systems equipment and resources.
- [Third Party Due Diligence Policy](#), when Stockland enters into arrangements with third parties, a due diligence assessment is completed for all potential Joint Venture partners, offshore service providers and other parties e.g. suppliers, contractors upon request or when a risk flag is raised.
- [Escalation Policy](#) requires incidents, whether a failure to follow policy and/or potential breaches of the law or regulations to be escalated, investigated, assessed and reported.
- Employee screening is conducted prior to commencement of employment

6. Employees' responsibility

Consistent with Stockland's "Three Lines of Defence" approach to Risk Management and Compliance, all functions and employees are responsible for managing risk through identification, assessment, and treatment of risks. Employees can play a critical role in preventing and detecting fraud, bribery and corruption and help minimise the likelihood of fraud occurring at Stockland. In particular, Employees should:

- **Understand** what fraud, bribery and corruption are by reading this policy and completing any further related training which might be offered by Stockland
- **Be aware** of their responsibilities, adhere to correct job procedures, Code of Conduct and other policies

- **Be transparent** in their stance against fraudulent, corrupt or unethical conduct or practice and be familiar with the Code of Conduct
- **Never:**
 - offer, request, or receive bribes of any kind to or from any person
 - help, encourage, conspire with, or ask another person to offer a bribe
 - Make, arrange, or direct the making of a facilitation payment
- **Always act in the best interests of Stockland** and not abuse their position for personal gain
- **Be continuously vigilant** to the potential for fraud and corruption
- **Report suspicious behaviour** and fraud vulnerabilities to their Line Manager, Group Risk, or in accordance with the Whistleblowing Policy
- **Co-operate** with assessment and management of fraud incidents

If an Employee is in doubt of his or her responsibilities, whether fraud, bribery or corruption has occurred, or he/she received pressure to provide a bribe or act dishonestly, he/she should always contact Group Risk for guidance.

7. Detecting Fraud, Bribery and Corruption

Employees should be alert to behaviour which may indicate fraud, bribery or corruption is taking place. Such behaviour could take any form, and may include:

- An Employee's resistance to take annual leave
- An Employee's living beyond his or her means
- Significant change in the behaviour of an Employee

If fraudulent or corrupt behaviour or attempted fraud is suspected, Employees should consider the following:

- Did the action or event result in a monetary benefit or other advantage being received by a person or related party who was not entitled to it?
- Was the action unlawful or illegal?
- Was deception or other concealment activities used?

Employees are strongly encouraged to report any situations where they suspect that fraud, bribery or corruption has occurred.

8. Reporting Fraud, Bribery and Corruption (Escalation Procedures)

Stockland is committed to providing an environment in which all Employees feel comfortable reporting incidents of fraud, bribery and corruption. Stockland is also committed to supporting people who report fraud and/or bribery and/or corruption or suspicions of fraud and/or bribery and/or corruption in good faith, regardless of whether any wrongdoing was identified. If an Employee is aware of or suspects suspicious activities, they should escalate the issue via one of the following channels as soon as possible:

- **To their Line Manager:** Report to the relevant line Manager and he/she should escalate to Group Compliance as per Stockland's Escalation Policy for assessment (see 9) and response (see 10)
- **To Group Compliance:** If an Employee does not feel comfortable making a report to their Line Manager (for example where the Line Manager is involved in the fraudulent activity), they can raise the matter directly with Group Compliance at compliance@stockland.com.au

If an Employee is not comfortable with reporting through Line Management or Group Compliance, they are encouraged to report the incident in accordance with the Whistleblowing Policy: See the Whistleblowing Policy for further details.

9. Fraud, Bribery and Corruption Assessment

The Group Risk Officer and the General Counsel will assess the situation, recommend a course of action and develop a management plan in consultation confidentially with People and Culture, and the line Manager. Employees should provide all relevant information to assist with the assessment where possible.

The Group Risk Officer will record all reports of suspected fraud, bribery or corruption, including evidence available to support the allegation. The General Counsel will notify the Executive Committee and the Audit Committee of the existence of such reports.

Fraud, bribery or corruption incidents that are reported in accordance with the Whistleblowing Policy will be managed in accordance with the terms of that Policy.

10. Responding to Fraud, Bribery and Corruption

As far as is possible and subject to legal and regulatory obligations, Stockland will endeavour to maintain the confidentiality of Employees in order to protect those people from reprisals or victimisation. There may be circumstances where the law enforcement agencies or regulators will be notified of the fraudulent conduct.

Where permitted by law, Stockland will seek the recovery of money or property stolen or fraudulently misappropriated, through:

- Relevant provisions of the proceeds of crime legislation in the jurisdiction in which the offence was committed

Civil remedies in the relevant jurisdiction in which the fraudulent activity was undertaken

11. Policy Compliance

Failure to comply with this Policy may result in substantial fines and penalties being imposed upon Stockland, and may expose Stockland and/or its Employees to civil or criminal liability or other financial or reputational damage. It may put our Australian Financial Services (AFS) licences and other business Licences at risk. Employees who breach this Policy may face disciplinary action up to and including dismissal.

Employees must adhere to Stockland's Escalation Policy in reporting any breach of this Policy that they are involved in, or become aware of, and do so in a timely manner.

12. Review

This Policy is reviewed and updated:

- When applicable and appropriate, including when there are changes in business practice, legislation and compliance obligations; and
- At least every 2 years.

13. Related Policies

[Whistleblower Policy](#)

[Code of Conduct](#)

[Securities Trading Policy](#)

[Government Relations Policy](#)

[Risk Management Policy](#)

[Compliance Framework](#)

[Conflicts of Interest Policy](#)

[Escalation Policy](#)

[Third Party Due Diligence Policy](#)

14. Contact for Questions

Please contact Group Compliance at compliance@stockland.com.au for questions on this document.

15. Document Control

Revision	Date	Owner	Description of changes
1.0	26 May 2015	Group Risk Officer	Board approval of Policy
1.1	24 August 2020	Group Risk Officer	Revised Policy approved by Board