# Group Fraud Policy

| | |
|---|---|
| Policy Level: | 1 |
| Accountable Executive: | Group Chief Financial Officer & EGM Finance & Commercial Services |
| Date Approved: | 13 June 2019 |
| Date Effective: | 13 June 2019 |

**auspost.com.au**

# Contents

# Statement of Policy

## Overview

Our reputation, success and sustainability as an organisation depends on not only what we do, but how we do it.

It is important for this reason that we always act with integrity and comply with applicable laws, regulations, codes, policies and procedures relating to fraud management.

## Rationale & Scope

This Group Fraud Policy (*the Policy*) sets out the corporation's intent in managing Fraud by:

- articulating Board and senior management commitment and responsibility to mitigate, detect and respond to fraudulent activities by implementing appropriate policies, procedures and controls;
- asserting that all workforce participants refrain from fraudulent conduct and report suspected or witnessed instances of fraudulent conduct; and
- providing a framework for investigation of suspected fraudulent conduct including the appropriateness of the APG's response.

This policy is a fundamental component of the Fraud Management Framework, and aligns with Australia Post's Risk Management Policy and other related policies. The policy is based on the Commonwealth Fraud Control Framework 2017, the Australian Standard Fraud and Corruption Control AS 8001-2008, and aligns to the Protective Security Policy Framework.

This policy does not cover Revenue Leakage that would not otherwise be Fraud. It is also not applicable for third party on third party fraud.

## Application

The policy applies to Australia Post Group and all of its workforce participants worldwide, who are defined as anyone who performs services for the Australia Post Group, or on its behalf, and includes:

- employees of any company in the Australia Post Group;
- contractors, consultants, licensees and agents (and their employees and subcontractors), who perform services for the Australia Post Group; and
- any other third parties performing services for or on behalf of the Australia Post Group.

The Australia Post Group means the Australian Postal Corporation, its subsidiaries, and all of its associated entities.

## Audience

All of Australia Post Group and its workforce participants.

## Policy Principles

The Australia Post Group:

- Has zero tolerance for Fraud.
- Requires workforce participants not to engage in Fraud.
- Is committed to deterring, preventing, detecting, and responding to fraudulent behaviour which is sought to be committed against, or may arise out of any part of our business or related activities inside and outside of Australia.
- Has Our Ethics which assists in preventing Fraud and specifically requires workforce participants to undertake awareness training. All workforce participants are responsible for reporting all suspected, attempted, or actual Fraud incidents in accordance with the Group Incident Management Policy. This includes incidents alleged to have been perpetrated by internal or external parties. In addition, all workforce participants are responsible for complying with the Group Conflicts of Interest Policy.
- Ensures that alleged cases of Fraud committed against the APG will be confidentially investigated. Appropriate consequence management will be taken against any person found to have acted fraudulently. Any damage/loss from Fraud incidents will be minimised, prosecutions may be made by relevant authorities, and learnings from such incidents will be maximised. APG reserves the right to refer matters of any suspected or detected Fraud to the relevant authorities.
- Requires risk assessments addressing Fraud to be documented for all major business initiatives, projects and business as usual operations.
- Will identify requirements to meet legal, statutory, regulatory, risk management or contractual obligations with regard to Fraud management, and monitor compliance of those requirements.

## Awareness, Training & Induction

Managers are responsible for ensuring training is completed, and effectively communicating the process of Fraud reporting to their employees. Our commitment extends to communicating our policy and associated guidelines to all workforce participants and APG will:

- make this policy available on the intranet and to subsidiaries and associated entities,
- provide training about your responsibilities, and
- regularly remind you about your responsibilities under the Policy.

## Enforcement & Monitoring

Management has accountability to enforce this policy and deal with intentional non-compliance through the Employee Counselling and Discipline Process (ECDP), and enforcement of terms and conditions outlined in agreements and contracts. Management is also responsible for ensuring that training is completed and effectively communicating Fraud related obligations to their teams. Recovery action will be taken, supported by Group Security and the APG Legal Team, where there is clear evidence of fraud and the likely benefits outweigh the cost involved.

## Breaches, Variations & Exemptions

Management may seek variation to policy requirements by seeking approval from the Policy Owner via the Policy Administrator. As requirements are largely specified by legal, statutory, regulatory, risk management or contractual obligations, compensating controls may be required. The standard procedures for requesting Policy Exemptions / Deviations must be followed in each case. Any incidents or breaches in relation to this Policy must be managed in accordance with APG's Group Incident Management Policy and Compliance Framework.

Any incidents or breaches in relation to this Policy must be managed in accordance with APG's Group Incident Management Policy and Compliance Framework.

Any behaviour that breaches this Policy will be managed through the applicable investigation and disciplinary processes. A proven breach may result in disciplinary action, up to and including termination. Individuals may also face further action from government authorities depending on circumstance.

Australia Post Group may take action under its contracts with its workforce participants to enforce the policy and deal with breaches.

## Reporting

All suspected fraudulent activity can be reported by:

- notifying their immediate manager or supervisor,
- contacting the Whistleblower hotline (1800 799 353) or whistleblower@auspost.com.au to speak anonymously (if preferred) to an independent, external service provider (as set out in the Whistleblower Policy and Our Ethics), and
- contacting Group Security locally or on the national number (1800 621 621).

All suspected Fraud must be escalated immediately and in accordance with the *Group Incident Management Policy* to ensure preservation and safeguarding of evidence.

Anyone raising concerns or reporting another's wrongdoing in relation to suspected fraudulent action will be supported. If concerns are raised in good faith under this policy, no workforce participant will suffer demotion, penalty or other adverse consequences.

## Review

This policy will be reviewed at least every three years or when there is a change to the legislation.

# Roles & Responsibilities

## Policy Governance

| Requirement | Responsible area/Role | Activities |
|---|---|---|
| The Board must report to the Shareholder Minister(s) on the implementation of governance frameworks, including Fraud, in the Annual Report. | Board of Directors | The Board will ensure appropriate governance mechanisms and Fraud control frameworks are in place. |
| Chief Risk Officer has delegated Board Responsibility as the Fraud Officer. | Chief Risk Officer | To oversee the application of the Policy and the Fraud and Risk Management Frameworks supporting it. |

## Policy Operation

| Requirement | Responsible area/Role | Activities |
|---|---|---|
| Identifying and managing the Fraud risks associated with their business objectives and strategic activities | Managers | Business leaders (first line) are accountable for the ownership and management of Fraud risks within their areas and across the value chain in line with risk appetite, with advice and guidance on the risk and control environment from first line Assurance functions. |
| Comply with regulatory obligations, policies and procedures. Undertake relevant training. | Workforce participants | All employees are responsible for reporting any potential or suspected incidents of Fraud and report any weaknesses or inadequate controls that could increase the risk of Fraud. |

## Policy Monitoring & Oversight

| Requirement | Responsible area/Role | Activities |
|---|---|---|
| Compliance | Group Security | Oversee and ensure APG compliance to the principles of the Policy and in accordance with the enterprise risk management framework. |
| Breach & Incident Reporting | Group Security | Undertake second line reviews, investigations and reporting for Fraud related matters in line with the Enterprise Fraud Management Framework to the Audit and Risk Committee. |
| Reviews to test policy implementation for validating compliance to this policy | Group Security | **Option** to undertake second line reviews and assurance activities to test policy implementation. |
| Periodic internal audit for compliance to the policy | Internal Audit | **Option** to undertake third line assurance activities to determine the level of compliance with the Policy and ensure Breaches and Incidents are realised and reported appropriately. |

# Glossary

| Term | Definition |
|---|---|
| APG | Australia Post Group (APG) is defined as the Australian Postal Corporation and its subsidiaries. |
| Fraud | Any intentional act by one or more individuals (internal and external), involving the use of deception or misrepresentation to obtain an unlawful advantage to the detriment of the Australia Post Group.<br>**Examples**:<br>Fraud can typically result in an actual or potential financial loss. Examples include, but are not limited to:<br>• misappropriation of funds, securities, stock, supplies or other assets including use of assets for private purposes,<br>• planning or causing a loss to or creating a liability for Australia Post by deception,<br>• impropriety in the handling or reporting of money or financial records,<br>• false invoicing for goods or services never rendered or backdating agreements,<br>• create or maintain artificial prices<br>• submission of exaggerated or wholly fictitious accident, harassment or injury claims,<br>• entering or engaging in fictitious transactions, and<br>• misuse of entitlements. |
| Revenue leakage | Revenue leakage is the unnoticed or unintended loss of revenue either through not billing (or under-billing) customers for products and services or loss of potential revenue through counterfeit Australia Post Group products sold by other parties. |
| Workforce participants | Workforce participants are defined as anyone who performs services for the Australia Post Group, or on its behalf, and includes:<br>• employees of any company in the Australia Post Group;<br>• contractors, consultants, licensees and agents (and their employees and subcontractors), who perform services for the Australia Post Group; and<br>• any other third parties performing services for or on behalf of the Australia Post Group. |
| Whistleblower Policy | The Australia Post Group procedure for reporting on any internal issues or problems which, by their nature or circumstance, cannot be raised through the standard reporting line (i.e. Business Unit Manager, escalating to Risk and Compliance). Any Whistleblower incidents are reported to an independent, external agency to be investigated without prejudice or conflict of interest. |

# Policy Administration

## Key Policy Information

| Administrative Area | Policy Information |
|---|---|
| Document Title | Group Fraud Policy |
| Policy Level | 1 |
| Version No | 1.0 |

## Policy Owners and Governance Forums

| Administrative Area | Owner / Forum |
|---|---|
| Accountable Executive | Group Chief Financial Officer & EGM Finance & Commercial Services |
| Policy Owner | Chief Risk Officer |
| Policy Administrator | General Manager Group Compliance |
| Policy Content Owner | Head of Security Operations |
| Review and Approval Body | Audit & Risk Committee (Endorse)<br>Board (Approve) |

## Key Dates

| Administrative Area | Date |
|---|---|
| Policy Approval Date | 13 June 2019 |
| Policy Effective Date | 13 June 2019 |
| Next scheduled review | June 2022 |