# Fraud Prevention Policy

## 1. Policy Purpose

Dexus has no tolerance for fraudulent behaviour and activity.

Dexus's Fraud Prevention Policy (**the Policy**) supports this stance by setting out the Group's principles and expectations of employees with regard to fraud prevention; and providing guidance on the identification of fraudulent activity or behaviour, fraud risk management and how to report suspected fraud.

## 2. Scope and application

This Policy applies to Dexus Directors and employees, including contractors and agents acting for or on behalf of Dexus (employees).

Employees are required to take all reasonable measures to prevent, detect and manage fraud risk; and to report any instances of fraud or suspected fraud.

All suspected fraud is fully investigated.

Where fraud has been committed, all efforts will be made to recover wrongfully obtained assets from fraudsters. Any employee who has intentionally committed or aided and abetted the commission of fraud against Dexus or its customers will face disciplinary action which could include termination of employment or negative impact on remuneration. Fraud is a serious criminal offence in Australia and if convicted, can result in imprisonment.

## 3. Policy principles

Dexus has no tolerance for any fraud committed by employees or any third party acting on behalf of or for Dexus.

Dexus has adopted the following principles in relation to fraud:

- Act fairly, honestly and in good faith.
- Identify and implement proactive fraud prevention and detection measures to reduce opportunities that could lead to fraud.
- Adopt and promote a culture of fraud awareness and effective management to ensure fraud issues are identified, investigated and reported.

Dexus is committed to giving effect to these principles by:

- Adopting relevant policies and operating processes and guidelines.
- Maintaining appropriate reporting and investigation processes and procedures.
- Conducting periodic reviews of fraud risk management arrangements, including policies and procedures.
- Providing general fraud awareness training to Dexus employees on an annual basis.

## 4. Definition of Fraud

Fraud is defined as a dishonest activity causing actual or potential gain or loss to any person or organisation, including theft of moneys or other property, by persons internal and/or external to the organisation and/or where deception is used at the time, immediately before or immediately following the activity (*per Australian Standard for Fraud and Corruption Control (AS 8001-2021)*).

Any fraudulent or attempted fraudulent conduct can originate internally or externally:

- ***Internal Fraud***: committed by a member of Dexus's staff or an authorised representative of a Dexus licensee.
- ***External Fraud***: committed by a person or persons who are external to Dexus. External fraud may include fraud committed by a Dexus customer or a third party such as an external advisor.

## 5. Reporting Fraud

Dexus requires all suspected or actual fraud related matters to be reported as soon as they are identified for a prompt investigation to determine the actions required. This may involve reporting to external parties such as law enforcement, regulators, or an investigative agency.

There are several channels to report instances of fraud or suspected fraud:

- Head of Risk
- Whistleblowing Protection Officers (refer to the *Whistleblower Policy*)

- Your-Call via the Your-Call website (yourcall.com.au) or call 1300 790 228 between 9:00am and midnight AEST (excluding weekends and public holidays) using Dexus' ID: DEXU500.
- Relevant Business Manager (where appropriate).

The following information should be provided when reporting a suspected or actual fraud:

- Date the incident was identified
- Date the incident occurred
- Brief description of the incident including how it was identified and how it occurred
- Details of the impact to client/funds, if any
- If the incident involved a supplier, other third party or external service provider
- Financial impact (if known).

Dexus strongly supports disclosure being made by employees of fraudulent conduct, illegality, or improper use of the company's assets. In the event the reporter wishes to remain anonymous, Dexus has established a Whistleblower Policy to protect those employees who make such disclosures from any detrimental action or reprisal.

## 6. Investigation

The Head of Risk will lead the investigation to determine the cause, nature and circumstances surrounding the incident or activity. The matter will be recorded as an incident and where it involves an employee of Dexus, the incident will be recorded as 'confidential'. The Head of Risk will advise the Executive Committee, Risk Committee and other Boards (where appropriate).

## 7. Fraud indicators and fraudulent conduct

Fraud indicators assist individuals in identifying instances of fraud or suspected fraud. Each indicator alone does not confirm fraudulent activity; however, they can serve as warning signs that warrant further investigation should they arise. Common fraud indicators and activities that constitute and facilitate fraud to be aware of include:

| Internal Fraud Indicators and Misconduct | Description |
|---|---|
| **Collusion** | Suspicious activities involving multiple employees collaborating to bypass controls, manipulate records, or facilitate fraudulent transactions. This could involve Dexus employees providing information or other assistance to third parties to help them commit fraud upon Dexus or a client of Dexus. |
| **Insider trading** | Buying or selling Dexus securities (including DXI, DXC and DXS[1]) based on non-public (inside) price sensitive information not generally available to investors breaches the *Corporations Act 2001*. The law prohibits the use of inside information (insider trading) and the disclosure of inside information (tipping). |
| **Forgery of records** | The falsifying of records and processing of a false statement is fraud e.g. falsifying data on receipts or invoices; forgery of a signature on a document; and forgery of certificates of competency or qualifications.<br>This includes the provision of financial information or reports to management, auditors, the Boards and their committees, regulatory authorities and to the public which are intentionally false. |
| **Misappropriation of assets and access** | Inappropriate use of the company's property and assets including (but not limited to) unauthorised usage of funds, facilities, confidential information, and intellectual property.<br>Unauthorised access to sensitive systems, unauthorised changes to user permissions can also expose vulnerabilities that facilitate fraud. |
| **Lack of segregation in duties** | When a single individual has control over multiple aspects of a process or transaction, it increases the risk of fraudulent activities, as there are fewer checks and balances in place. Fraudulent behaviour an employee may exhibit |

[1] DXI = Dexus Industria REIT™; DXC = Dexus Convenience Retail REIT; and DXS = Dexus Property Group all of which are listed on the Australian Stock Exchange (ASX).

| | |
|---|---|
| | includes unwillingness to take leave or share duties and excessive control without reasonable explanation |
| **Conflicts of Interest** | Accepting commissions, fees, gifts or favours that might act as an inducement to do business or influence a business decision could result in a conflict of interest. Conflicts of interest must be reported immediately to Compliance to ensure appropriate management of the actual or potential conflict. |
| **Deceptive conduct** | Any act, behaviour or statement made with the intention of misleading another party to enter into a contractual or business arrangement or procure/purchase a product or service which is inappropriate or unsuitable for their circumstances and may result in monetary loss or inadequate benefits for price/cost incurred. |

| External Fraud Indicators | Description |
|---|---|
| **Unusual transactions** | Large or frequent transactions that are inconsistent with a customer's normal behaviour or transaction patterns can indicate potential fraud. |
| **Customer complaints or anomalies** | Frequent complaints from customers about incorrect or unauthorised transactions, unexplained fees, or unusual account activities should be investigated further. |
| **Supplier or other third-party invoice changes** | Supplier or third-party invoices may indicate fraudulent activity if the invoice:<br>• Includes insufficient detail to support payment; or<br>• Amount has increased significantly with no discernible change in contracted terms; or<br>• Bank account details for payment have changed without previous notification from the supplier or other third party. |
| **Failed security verification checks** | The individual claiming to be the customer repeatedly fails security checks when requesting a redemption or changes to their static data such as their bank account details. |

## 8. Fraud risk management

The fraud risk management approach at Dexus follows the *Risk Management Framework* and is underpinned by the following principles:

- ***Fraud prevention**:* includes the establishment of an appropriate risk culture that promotes ethical behaviour across all levels of staff at Dexus and implementation of proactive controls to prevent incidents of fraud. Proactive preventative controls are periodic measures designed to actively seek out evidence of fraudulent activity and allow objective assessment of the effectiveness of the fraud risk controls in place. Fraud awareness training is also provided to all staff on an annual basis.
- ***Fraud detection**:* can take place through various channels including internal monitoring activities, external reviews, complaints received or whistleblowing. Dexus employs reactive detection controls which are designed to identify indicators of fraud and to detect occurrences of fraud. The Risk team facilitates risk assessments on an annual basis to assist with identifying fraud risk within the various business units and implementing treatment plans to mitigate the risk.
- ***Fraud response**:* Dexus ensures timely investigation and response to detected fraud by identifying the associated risk and treatment plans based on determined facts.
- ***Monitoring and review**:* annual risk assessments, regular monitoring and review of fraud risk controls will ensure the risk and control environment remains appropriate and continue to address identified fraud risks or any emerging risks identified during the review.

## 9. Roles and Responsibilities

| Role | Responsibility |
|---|---|
| All employees | Taking all measures to prevent fraudulent activity and report any suspected |

| | |
|---|---|
| | fraudulent activity or behaviour immediately. Including:<br>– Knowing what fraud is, being familiar with this policy and completing fraud prevention training<br>– Understanding the responsibilities of their position; familiarising themselves with correct job procedures and adhering to them<br>– Being aware of strategies implemented in their team / business unit to minimise the risk of fraud<br>– Being continuously vigilant to the potential for fraud, alerting responsible people to possible or perceived vulnerabilities.<br>– Assist with investigation of fraud where appropriate. |
| Risk Team | – Raising awareness of fraud<br>– Planning, execution and ongoing maintenance of Fraud Prevention Policy, including periodic fraud internal audits at least every 3 years<br>– Implementing monitoring activities for fraud indicators<br>– Leading any suspected fraud investigations. |
| Executive Committee | – Establishing an appropriate risk culture that promotes ethical behaviour<br>– To ensure appropriate risk and compliance management practices and policies are in place to prevent and manage fraud<br>– Assist with investigation of fraud where appropriate. |
| Dexus Board Risk Committee | – Reviewing all incidents of reported fraud<br>– Assist with investigation of fraud where appropriate. |
| Dexus Board of Directors | – Awareness and management of significant instances of fraud. |

## 10. Training and awareness

Fraud awareness training is provided to all staff on an annual basis via training courses and regular communication to employees.

## 11. Governance

The Policy is owned by the Risk team and is approved by the Board Risk Committee (BRC) following review and endorsement by the Group Management Committee (GMC) on an annual basis.

## 12. Additional Information

If you have any questions arising from this Policy, please contact - Natalie Wray, Head of Risk

## 13. Related Policies

This policy should be read in conjunction with the Risk Management Framework and the following related policies and programs:

- Employee Code of Conduct.
- Conflicts of Interest and Related Party Transactions Policy.
- Whistleblower Policy.
- Joint Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Programs.
- Anti-Bribery and Corruption (ABC) Policy.
- Sanctions Policy.
- Compliance Incident and Breach Management Policy.
- Securities Trading Policy (including Inside Information).
- Workplace Behaviour Policy.

## 14. Document Control Log

| Version | Document Owner | Author | Approving Authority | Approved Date |
|---|---|---|---|---|
| *Formerly subset of "Fraud, Corruption & Bribery" Policy, V14* | Compliance | Rachel Caralis | Corporate Executive Committee<br>Board Risk Committee | 16 May 2023<br>6 June 2023 |
| 1 | Head of Risk | Andrew Pietor | Executive Committee<br>Board Risk Committee | 25 September 2023<br>17 November 2023 |