Dornan Engineering Limited its Subsidiaries and Branches
Hereafter for the purpose of this Policy known as **Dornan**
c

# ANTI-FRAUD POLICY

**NOVEMBER 2025**

## CONTENTS

# ANTI-FRAUD POLICY

## 1. PURPOSE

This Anti-Fraud Compliance Policy ("Policy") establishes Dornan's commitment to conducting business with integrity and in compliance with applicable anti-fraud laws, including the Economic Crime and Corporate Transparency Act 2023 Failure to Prevent Fraud (the "FTPF").

Dornan maintains a zero-tolerance approach to Fraud or any form of dishonest or unethical conduct. This means that any act of deception, misrepresentation, theft, embezzlement, forgery, or abuse of position for personal or corporate gain is strictly prohibited, regardless of the amount or perceived impact.

All Employees, Business Partners, and Associated Persons acting on behalf of Dornan must act with honesty, integrity, and transparency at all times. It is the responsibility of every individual to safeguard the company's assets and reputation by adhering to the highest ethical standards in all business dealings.

Any Employee, Business Partners or associated person who suspects or becomes aware of fraudulent activity, Attempted Fraud, or any suspicious behaviour must report their concerns immediately. Reports can be made directly to the Legal, Compliance and Data Protection Department (the "LCD"), line management, or through Dornan's confidential whistleblowing channel. All reports will be treated seriously and investigated promptly, with strict confidentiality maintained to protect those raising concerns in good faith.

Dornan prohibits retaliation against anyone who, in good faith, reports suspected Fraud or participates in an investigation. Disciplinary action, up to and including dismissal, may be taken against anyone found to have committed or facilitated Fraud, or who fails to report such activity.

Dornan ensures all necessary steps to prevent, detect, and respond to Fraud, including but not limited to maintaining robust internal controls, providing regular anti-fraud training, and cooperating fully with law enforcement and regulatory authorities as required.

## 2. SCOPE

This Policy applies to all Dornan Employees, Business Partners and Associated Persons acting on behalf of Dornan, across all locations and subsidiaries.

## 3. DEFINITIONS

| | |
|---|---|
| Fraud | Any act of dishonesty or deception intended to secure an unlawful gain or cause a loss, including false representations, failure to disclose information, and abuse of position. |
| Attempted Fraud | Behaviour that indicates a risk of Fraud (including but not limited to pressure to bypass controls, unusual supplier bank changes, duplicate invoicing). |
| Business Partners/Associated Persons | Any individual or entity engaged in a business relationship with the company, including but not limited to suppliers, contractors, subcontractors, consultants, agents, intermediaries, and any third parties acting on behalf of the company and/or any individual or entity that performs services for or on behalf of the company, regardless of the nature of the relationship whose actions could expose the company to fraud or corruption risk. |
| Employees | Any individual engaged under a contract of employment with the company, including permanent, fixed-term, temporary, and casual staff, as well as interns and trainees where applicable. |

## 4. RESPONSIBILITIES

**Senior Management and Board of Directors (Accountable)**

Holds overall responsibility for anti-fraud governance. The Board sets the tone from the top and the Senior Management approves this Policy and ensures that adequate resources and oversight mechanisms are in place to prevent and respond to Fraud.

**Legal, Compliance and Data Protection Department (Responsible)**

Oversees the implementation of this Policy, delivers anti-fraud training, maintains the Fraud Incident Log, and leads independent investigations into suspected Fraud. The LCD also monitors legislative changes, reviews internal controls, and reports regularly to the Board and Senior Management.

**Managers (Responsible/Consulted)**

Promote a culture of integrity within their teams, ensure that anti-fraud controls are embedded in daily operations, and support investigations as required. Managers are accountable for ensuring their teams understand the escalation process, comply fully with this Policy, and promptly escalate any concerns to the LCD Department.

**All Employees, Business Partners and Associated Persons (Responsible/Informed)**

Employees, Business Partners and Associated Persons must act honestly, comply with this Policy, attend mandatory anti-fraud training, and promptly report any suspected fraudulent activity or suspicious behaviour. All of the above are encouraged to use Dornan's confidential whistleblowing channel and are protected from retaliation when reporting in good faith.

## 5. PREVENTION AND CONTROLS

Dornan is committed to maintaining a robust framework of preventive measures to mitigate the risk of Fraud across all areas of operation. These controls are aligned with the UK Government's six principles for reasonable Fraud prevention procedures and reflect Dornan's ISO-aligned Compliance Management System (CMS) and Anti-Bribery Management System (ABMS).

### 5.1. INTERNAL CONTROLS AND OVERSIGHT

- Maintain documented internal controls across all functions of the business.
- Ensure segregation of duties and internal procedures are applied in high-risk areas such as, but not limited to bidding, change orders, ESG reporting, and progress claims, in line with internal governance procedures.
- Conduct regular internal audits and compliance reviews to test control effectiveness and identify gaps.

### 5.2. DUE DILIGENCE ON THIRD PARTIES

- Apply Dornan's Business Partners Risk Matrix to classify subcontractors and suppliers by risk level.
- Require high-risk Business Partners to undergo enhanced due diligence, including pre-qualification assessments and compliance monitoring, as set out in the
- Mandate signing of Dornan's Code of Conduct for Business Partners and inclusion of anti-fraud clauses in contracts.

### 5.3. CONTRACTUAL SAFEGUARDS

- Embed anti-fraud warranties and notification duties in all UK-project templates and high-risk contracts.
- Include rights to audit, terminate, and require training in third-party agreements.
- Ensure all contractual language reflects Dornan's zero-tolerance stance and legal obligations under the UK Economic Crime and Corporate Transparency Act 2023 (ECCTA), Irish Criminal Justice (Corruption Offences) Act, and relevant EU directives

### 5.4. TRAINING AND AWARENESS

- Anti-fraud training is included as part of Dornan's weekly induction training for all new Employees, ensuring that awareness of Fraud risks and prevention measures is established from the outset.
- Ongoing anti-fraud training and fraud prevention are provided to all Employees in line with local legislative requirements and Dornan's commitment to compliance.

### 5.5. LEGISLATIVE MONITORING

- Monitor changes in fraud-related legislation across all jurisdictions where Dornan operates.
- Update policies and procedures in response to new laws, including but not limited to the UK Failure to Prevent Fraud offence.
- Maintain a central compliance tracker to document legislative changes, risk assessments, and control updates.

### 5.6. CONTINUOUS IMPROVEMENT

Dornan reviews and enhances its fraud-prevention controls on an ongoing basis to ensure they remain effective, risk-based, and proportionate. Reviews are conducted at least annually and following any incident, audit finding, or material change in operations or law. Cross-functional working groups assess emerging risks and recommend control enhancements, and effectiveness metrics (including, but not limited to, training completion rates, audit action closure rates, and incident response times) are reported to the Board, Senior Management, and the Compliance Committee.

### 5.7. REAL-WORLD CONSTRUCTION FRAUD SCENARIOS (INDUSTRY ENFORCEMENT SNAPSHOTS)

These anonymised, industry-relevant examples are for guidance only and are not exhaustive. If in doubt, pause and escalate in accordance with Section 7 of this Policy. For details on disciplinary and legal outcomes, refer to Section 8 of this Policy.

### CASE 1: ILLEGAL BID RIGGING - £60 MILLION IN FINES

In March 2023, ten major UK construction firms were fined nearly £60 million for colluding on demolition and asbestos removal contracts. They manipulated tender outcomes for high-profile projects, including Oxford University and Selfridges, artificially inflating costs and undermining fair competition.

**Key Fraud elements includes:**

- Bid rigging (coordinated bids to distort competition);
- Market manipulation (secured contracts unfairly through collusion);
- Public Impact (Increased costs for taxpayers and clients).

The Competition and Markets Authority imposed corporate penalties totalling £60 million, underscoring the seriousness of bid rigging. In addition to financial sanctions, three directors faced personal liability through disqualification for up to 7.5 years. Beyond these legal and financial repercussions, the case inflicted significant reputational damage, with the CMA emphasising that collusive practices erode trust and inflate costs across the industry.

Collusion in procurement exposes organisations to severe financial penalties, leadership disqualification, and lasting reputational harm. This case highlights the critical need for robust tendering controls, transparent processes, and comprehensive compliance training to prevent similar misconduct and protect corporate integrity.

### CASE 2: PAYROLL & TAX FRAUD - £22 MILLION SCHEME

In February 2025, seven individuals, including payroll administrators and a construction company director were convicted for orchestrating a £22 million tax and employment fraud. They created fake payroll companies issuing invoices with VAT and CIS deductions that were never paid to HMRC. Funds were diverted to personal accounts.

**Key Fraud elements includes:**

- False Payroll Structures (fake companies simulating legitimate employment);
- Kickbacks (cash incentives to route business to fraudulent firms);
- Money Laundering (cash couriers moved illicit funds through personal accounts);
- Cheating the Revenue: (millions lost in employment-related taxes).

The individuals involved faced serious criminal penalties, with sentences ranging from two years suspended to nine years and four months of imprisonment. Convictions included

offences such as cheating the revenue, money laundering, and acquiring criminal property, reflecting the gravity of the scheme and its impact on financial integrity.

This case underscores significant failures in subcontractor vetting and payroll oversight. It highlights the importance of strong due diligence processes and continuous monitoring to prevent similar fraudulent schemes and protect organisational compliance.

## 6. TECHNOLOGY AND CYBER-FRAUD

For activities within scope of the UK Economic Crime and Corporate Transparency Act 2023 "Failure to Prevent Fraud" offence, Dornan implements and continually improves reasonable fraud-prevention procedures. Our fraud risk assessment explicitly considers cyber-enabled methods by which base fraud offences may be committed (to include but not limited to phishing and social-engineering; business email compromise and fraudulent payment-detail changes; credential theft and unauthorised system access; malware/ransomware used to misdirect or extort funds).

### 6.1. CYBER FRAUD CONTROLS

**Phishing and Social Engineering**

All Employees must remain vigilant against phishing attempts, social engineering, and fraudulent communications.

**Payment-instruction verification**

All Employees must independently confirm channels before any bank-detail changes or unusual transfers.

**Business Email Compromise**

Dornan enforces strict verification procedures for financial transactions and changes to supplier or payment details. Employees must confirm such requests through independent channels before taking action.

**Cyber-Enabled Fraud**

The company monitors for cyber threats such as malware, ransomware, and unauthorised access to systems or data. IT security protocols, including multi-factor authentication and regular system updates, are mandatory.

### 6.2. SECURE HANDLING OF SENSITIVE INFORMATION

Employees must follow company guidelines for the secure storage, transmission, and disposal of sensitive data, including personal, financial, and confidential business information.

Access to sensitive systems and data is restricted to authorised personnel only, and usage is monitored for unusual or unauthorised activity.

### 6.3. REPORTING SUSPECTED CYBER INCIDENTS

Any suspected cyber-Fraud, including phishing attempts, suspicious emails, or unauthorised access to company systems, must be reported immediately to the IT Security Team and/or to the Data Protection Officer. Dornan maintains a confidential reporting channel for cyber incidents, and all reports will be investigated promptly and confidentially. Employees are encouraged to report incidents without fear of retaliation, in line with Dornan's whistleblowing procedures.

## 7. REPORTING AND WHISTLEBLOWING

All suspected Fraud must be reported immediately to the LCD or through Dornan's confidential whistleblowing channel. Reports may be submitted internally and externally via compliance@dornangroup.com.

All reports will be acknowledged within 7 days and investigated promptly, confidentially, and impartially in accordance with the EEA and the UK legislation. Where Fraud is found to have been committed or facilitated, disciplinary action may be taken, up to and including dismissal. Dornan will also cooperate fully with law enforcement and regulatory authorities as required.

Dornan maintains a strict non-retaliation commitment to protect individuals who report concerns in good faith.

## 8. CONSEQUENCES OF NON-COMPLIANCE

The table below outlines the potential consequences of non-compliance with fraud legislation within the UK and EU/EEA. This list is not exhaustive.

| Category | Key Consequences | Relevant Legislation | Penalties/Sanctions |
|---|---|---|---|
| **Employees** | • Disciplinary action up to and including dismissal<br>• Criminal prosecution for | • UK Fraud Act 2006<br>• EU PIF Directive | • Up to 10 years in prison<br>• Fines (unlimited for serious offences) |

| | | | |
|---|---|---|---|
| | fraud, bribery, tax evasion<br>• Loss of professional accreditation | • EU Public Procurement Directive 2014<br>• EU AML Directive 2018 | • Minimum 4 years imprisonment for AML offences |
| **Top Management** | • Personal criminal liability for consent/connivance<br>• Director disqualification<br>• Asset confiscation | • UK ECCTA 2023 (Failure to Prevent Fraud)<br>• UK Bribery Act 2010<br>• EU OLAF Regulation | • Unlimited fines for corporate offences<br>• Disqualification up to 15 years under Company Directors Disqualification Act<br>• Confiscation of assets; imprisonment in default |
| **Overall company** | • Unlimited fines<br>• Criminal convictions<br>• Exclusion from public procurement<br>• Serious reputational damage<br>• Loss of Projects | • UK ECCTA 2023.<br>• UK Bribery Act 2010<br>• EU Procurement Directive 2014 | • Unlimited fines<br>• Debarment<br>• Criminal liability |

## 9. INTEGRATION WITH OTHER POLICIES

This Policy is designed to operate in harmony with other key governance and all compliance policies. It supports a unified approach to ethical conduct, risk management, and legal compliance across all operations. The Anti-Fraud Policy compliments this framework by reinforcing Dornan's commitment to integrity and transparency and by strengthening existing anti-bribery and corruption controls.

## 10. REVIEW

This Policy will be subject to a formal review on an annual basis to ensure its continued relevance, effectiveness, and alignment with applicable legal and regulatory requirements,

including anti-fraud legislation, data protection laws, and corporate governance standards. In addition to the scheduled annual review, an ad hoc review will be triggered whenever there are significant changes in legislation, regulatory guidance, industry best practice, organisational structure, business operations, or risk profile that could impact the policy's adequacy or implementation.