



STATOM HOLDINGS Limited (Statom Group Limited, Statom Group North Ltd, Statom Plant Ltd, Statom Remediation Ltd, Demoforce Group Ltd, FL-Facilities Group Ltd, Slipform Technology Ltd, Spark Tech MEP Ltd, Franki Foundations UK Ltd, Martello Piling Ltd) (“Statom”, “the Company”)

We are committed to high standards of professional conduct, integrity and accountability. As a leading civil engineering and construction organisation, we recognise that the behaviour and standards of our people are fundamental to building a strong, respectful culture and protecting our reputation as a trusted industry leader.

We expect everyone working for or on behalf of the Company to act with professionalism, respect and responsibility at all times, reflecting our values and supporting a positive working environment. Clear standards of behaviour are essential to ensuring safety, quality and effective collaboration across our projects and teams.

1. Purpose

This policy sets the Group framework for preventing, detecting, reporting and responding to fraud. It reflects the Fraud Act 2006 and the corporate failure-to-prevent-fraud offence created by the Economic Crime and Corporate Transparency Act 2023, which has been in force since 1 September 2025.

2. Scope

It applies to all employees, directors, officers, workers, agency workers, consultants, contractors, suppliers, agents, intermediaries and other persons performing services for or on behalf of Statom Group.

3. Fraud and the Corporate Offence

Fraud includes dishonest false representation, failure to disclose information where there is a legal duty to disclose it, abuse of position, false accounting, fraudulent trading and other specified fraud offences. Under the failure-to-prevent-fraud regime, a qualifying large organisation may be criminally liable where an associated person commits a specified fraud offence intending to benefit the organisation or certain connected persons and the organisation did not have reasonable fraud prevention procedures.

4. Zero-Tolerance Standard

- No person may falsify, manipulate or conceal financial, payroll, timesheet, procurement, tender, expense, project, quality, safety, competence or compliance records.
- No person may create fictitious suppliers, invoices, employees, subcontractors, variations, claims, rebates or payments.
- No person may misuse Company assets, cards, accounts, systems, confidential information or delegated authority for personal or third-party gain.
- No manager may encourage, approve or ignore dishonest conduct to achieve commercial, project, revenue, margin, bonus or tender outcomes.

5. Reasonable Fraud Prevention Procedures

- top-level commitment and clear accountability;
- documented fraud risk assessments covering business units, projects, payments, procurement, payroll, CIS, expenses, suppliers and third parties;
- proportionate controls including segregation of duties, approval limits, supplier validation, bank-detail change verification, reconciliations and audit trails;
- risk-based due diligence on associated persons and counterparties;
- training and communication targeted to exposure; and
- monitoring, testing, incident learning and periodic review.

6. Reporting and Whistleblowing

Suspected fraud must be reported immediately to the Chief People Officer, Finance Director, a Group Director or under the Whistleblowing Policy. Reports may be made confidentially. No person will suffer retaliation for raising a genuine concern or assisting an investigation.

7. Investigation Controls

Investigations will be independent and proportionate. The Company may preserve emails, system logs, financial records, devices, CCTV and other evidence in accordance with law and Company policy. Individuals must not alert a suspected wrongdoer, destroy evidence or conduct unauthorised investigations. Legal privilege, data protection, fairness and disciplinary procedure requirements will be respected.

8. Response and Recovery

Where fraud is established or reasonably suspected, the Company may take disciplinary or contractual action, suspend access or payments, seek recovery, notify insurers, clients, auditors or regulators where required, and refer matters to law enforcement. Decisions will be documented.

9. Records and Assurance

Fraud risk assessments, prevention measures, training, reports, investigations and remediation actions must be recorded sufficiently to demonstrate the operation of reasonable procedures. Material risks and incidents will be escalated to the Board.

10. Related Policies

Related documents include the Anti-Bribery and Anti-Corruption Policy, Anti-Tax Evasion Policy, AML and Counter-Terrorist Financing Policy, Conflict of Interest Policy, Whistleblowing Policy, Expenses Policy, Data Protection Policy and Disciplinary Policy.

Approval and Review

This policy will be reviewed at least annually and earlier where legislation, regulatory guidance, case law, Company structure, operational risk or business practice changes materially. Substantive amendments require appropriate Group approval before issue.

AUTHORISED AND APPROVED

SIGNED



Gavin Hunt
Chief Development Officer

Review: Annually
Date: 01/06/2026
Next Review: 01/06/2027

SIGNED



Martina Oyite
Chief People Officer

Review: Annually
Date: 01/06/2026
Next Review: 01/06/2027

*Review: Annually or earlier where legislation, guidance, Company practice or operational requirements change.
This policy is subject to annual review and approval by the Board.*