FRAUD PREVENTION POLICY STATEMENT

Bachy Soletanche Ltd (BSL) is a specialist geotechnical contractor providing ground investigation, foundation, and geotechnical solutions for the construction industry. This Policy explains the arrangements Bachy Soletanche Limited has in place to prevent, detect, report and respond to fraud and attempted fraud. It supports the VINCI commitment to conduct business fairly, honestly and openly, recognises the financial and reputational harm fraud can cause, and confirms a zero-tolerance approach to fraud.

The Policy also describes how the Company assesses fraud risk, assigns responsibilities, applies proportionate controls, trains relevant personnel, monitors effectiveness and improves its arrangements.

Scope and Alignment

This Policy applies to all directors, employees, agency workers and other persons providing services for or on behalf of the Company, including subsidiaries where applicable, agents, subcontractors, consultants and other members of the supply chain. These persons are referred to in this Policy as “associated persons” or the “workforce”, as the context requires.

It applies across the Company’s business activities, projects, offices, systems, transactions and records. The main legal and governance focus is fraud committed by, or on behalf of, the Company or an associated person with an intention to benefit the Company or a person receiving services from that associated person.

Fraud committed against the Company is managed through the applicable VINCI Fraud Prevention Handbook, security, cyber, finance and incident-response arrangements. Suspected external fraud must still be reported promptly under section 10 of this Policy.

This Policy supplements VINCI SA document AUD 4-1, Preventing and Combating Fraud at VINCI SA, and the VINCI Construction UK Fraud Prevention Policy. Where a Group requirement is stricter than this Policy, the Group requirement takes precedence.

Definitions of Fraud

Fraud is a criminal offence involving deception used dishonestly to make a gain for oneself or another person, or to cause or expose another person or organisation to loss.

- Fraud by false representation.
- Fraud by failing to disclose information when there is a legal duty to disclose it.
- Fraud by abuse of position.

Key terms

- Attempted fraud: Fraudulent activity detected or prevented before a loss or intended benefit occurs.
- Red flag: An indicator that may warrant further checking, such as an unusual payment request, duplicate supplier information or missing evidence.
- Associated person: A person or organisation providing services for or on behalf of the Company, including employees, agents, subcontractors, consultants and relevant supply-chain members.
- Third party: A supplier, subcontractor, agent, consultant or other business partner.

Failure to Prevent Fraud

In addition to the liability of an individual who commits an offence, a large organisation may be criminally liable where an associated person commits a relevant fraud offence intending to benefit the organisation or a person to whom the associated person provides services on the organisation’s behalf. The Company

therefore maintains reasonable, risk-based prevention procedures and evidence that these procedures are implemented in practice.

Governance Roles and Responsibilities

- Board / senior management: Set the tone from the top; approve the Policy; provide appropriate resources; consider fraud-risk reporting; challenge significant weaknesses and overdue actions.
- Policy owner: Maintain the Policy; coordinate risk assessment, training and monitoring; retain evidence; report material risks, incidents and actions to senior management.
- Line managers: Embed relevant controls; ensure required training is completed; review exceptions; escalate concerns promptly; support investigations and corrective actions.
- Finance, Procurement, HR and IT: Design, operate and evidence controls in their areas, including payment, supplier, payroll, access, logging and data-integrity controls.
- All workforce members: Act honestly; comply with controls; remain alert to red flags; protect assets, information and records; declare conflicts; report concerns promptly; preserve evidence.
- Associated persons / third parties: Comply with contractual requirements and applicable Company policies; maintain accurate records; cooperate with due diligence, monitoring and investigations.

Fraud Prevention Procedure

Governance and culture

- Zero tolerance of fraud, attempted fraud, concealment and retaliation against anyone reporting a concern in good faith.
- Clear reporting routes and prompt, appropriately independent investigation of concerns.
- Segregation of duties so that, where practicable, no single person can create, approve and complete a transaction end-to-end.
- Proportionate pre-employment screening for roles with financial authority, sensitive information or privileged system access.
- Documented approval authorities, delegated limits and accountability for control ownership.

Finance and payment controls

- Payments require approval in accordance with the current delegated authority and approval matrix.
- Supplier bank-detail changes are independently verified using a known, previously verified contact route before records are amended.
- Invoices are matched to purchase orders and evidence of receipt or performance where applicable; a three-way match is used where practicable.
- The person creating a supplier or initiating a payment is not the same person approving it, where practicable.
- Bank and key control accounts are reconciled regularly and independently reviewed.
- Transactions are supported by accurate, complete and retrievable records. Backdating, falsification and deliberate concealment are prohibited.

Procurement and third-party controls

- Proportionate due diligence is completed before onboarding and refreshed where risk or circumstances justify it, including identity, ownership and relevant integrity checks.
- Material expenditure is supported by written contracts or purchase terms covering scope, price and appropriate audit, suspension or termination rights.
- Actual, potential or perceived conflicts of interest are declared and managed.
- Competitive quotations or tendering are used in accordance with internal thresholds, with the selection rationale retained.
- Cash payments are prohibited unless expressly authorised, recorded and supported by receipts.
- Relevant associated persons receive clear contractual expectations concerning fraud prevention, records, cooperation and reporting.

Payroll, HR, expenses and purchasing cards

- Starters, leavers and role changes are authorised and reflected promptly in payroll and system access.
- Employee bank-detail and material pay changes are independently verified and authorised before implementation.
- Overtime, expenses and allowances require appropriate approval and supporting evidence.
- Payroll preparation and payment release are separated where practicable; exception reports are reviewed.
- Expense claims must be timely, reasonable, business-related and supported by itemised evidence.
- Purchasing cards have defined users, limits and permitted categories, with periodic review of statements and receipts.

IT, data and cyber-enabled fraud controls

- Access is role-based, approved, periodically reviewed and removed promptly following a role change or exit.
- Multi-factor authentication is used where available for finance, email, remote access and other sensitive systems.
- Key systems retain appropriate logs and audit trails for user activity, approvals and master-data changes.
- Unusual or urgent payment requests, including senior-person impersonation, are independently verified and suspected phishing is reported immediately.
- Critical records are backed up and protected from unauthorised access, alteration or deletion.

Fraud Risk Assessment

The Company will participate in and support the Group fraud-risk assessment cycle. In line with the Group strategy, each relevant UK delegation and shared service department carries out a fraud risk assessment every two years, with a review in the intervening year. The Company will also review relevant risks when

significant changes occur, such as new systems, new services, acquisitions, significant suppliers, new payment methods or material incidents.

The assessment will consider fraud by the Company and fraud carried out on its behalf by associated persons. It will identify inherent risks, existing controls, residual exposure, actions, owners and completion dates. The assessment and review must be evidenced through an approved risk register, minutes and an action tracker.

Risk area	Illustrative risk	Key control themes
Payments	Supplier impersonation or fraudulent bank-detail change	Independent call-back; approval matrix; dual authorisation
Procurement	Kickbacks, collusion or undisclosed conflicts	Competitive sourcing; declarations; due diligence; segregation
Payroll	Ghost workers or unauthorised pay changes	Starter/leaver controls; payroll review; access restrictions
Expenses	False, duplicate or inflated claims	Receipts; manager approval; analytics or sample checks
Project / commercial	False records, valuation manipulation or dishonest claims	Defined authority; independent review; supporting records; audit trail
IT / cyber	Credential theft enabling payment or data fraud	MFA; phishing reporting; least privilege; logging

Training and Communication

Fraud-prevention training will be proportionate to role and risk. Relevant content will be included at induction and refreshed periodically, with more targeted training for higher-risk roles. Training and communications may cover:

- Policy expectations, reporting routes and common red flags.
- Invoice fraud, supplier-change verification, approval limits and reconciliations for Finance.
- Conflicts, gifts and hospitality, tender integrity and due diligence for Procurement and commercial roles.
- Starter/leaver controls and secure handling of personal and bank data for HR and Payroll.
- Phishing, impersonation fraud, password security and multi-factor authentication.
- Periodic alerts on emerging threats and lessons identified from incidents or near misses.

Attendance, completion and communication evidence will be retained, including learning-system reports, attendance logs, briefings, agendas and issued communications.

Monitoring, Assurance and Continuous Improvement

Monitoring is risk-based and is used to confirm that controls operate as intended, detect emerging risks and drive improvement. Activities may include:

- Review of payment runs and unusual transactions, new suppliers, duplicate bank accounts and out-of-pattern activity.

- Exception reporting for duplicate invoices, split purchases, sequential invoice patterns and changes to supplier or employee data.
- Independent review of reconciliations and key control-account sign-off.
- Periodic access reviews for finance, payroll and other sensitive systems.
- Sample testing or internal audit of expenses, procurement files, supplier due diligence and control evidence.
- Root-cause review of incidents and near misses, with corrective actions tracked to closure.
- Periodic reporting to senior management on material risks, incidents, weaknesses, overdue actions and assurance results.

A control is not fully demonstrable unless the Company can show who performed it, when it was performed, what was reviewed, the outcome and how any action was closed.

Reporting and Responding to Incidents

Anyone who knows, suspects, or reasonably believes that fraud has occurred or is likely to occur must report their concerns promptly. Where it is safe to do so and within their authority, individuals should take immediate steps to prevent further loss or damage, such as pausing a payment or transaction. Employees must not conduct their own investigation or alert any person suspected of involvement.

Actions required:

- Report any known, suspected, or potential fraud without delay.
- Take authorised and safe action to prevent further loss where appropriate.
- Do not investigate the matter yourself.
- Do not inform or confront the suspected individual.
- Maintain confidentiality and cooperate with any subsequent investigation.

Concerns should normally be reported to the UK Division Chief Financial Officer, who will escalate the matter confidentially to the appropriate Managing Director, Division Legal Counsel and Chief Executive, as required. Where an employee does not feel able to use this reporting route, concerns may be raised through the confidential external whistleblowing hotline, Safecall, on **0800 915 1571**.

Reporting routes:

- Report concerns to the UK Division Chief Financial Officer.
- Use the confidential Safecall hotline (0800 915 1571) if you feel unable to report through normal management channels.
- Follow any locally approved reporting or whistleblowing procedures once published.

Confidentiality, Protection and Evidence

- Reports will be handled sensitively and shared only with those who need the information for assessment, investigation or action.
- Retaliation against a person raising a concern in good faith is prohibited.
- Relevant emails, messages, records, devices and audit trails must be preserved. No one may delete, alter or conceal potential evidence.
- Investigations will be authorised and managed by appropriate persons, with Legal, HR, Finance, IT, Internal Audit, insurers, external specialists or authorities involved where appropriate.
- Any regulatory, client, insurer or law-enforcement notification will be managed by authorised functions.

Breaches and Consequences

Breach of this Policy may result in disciplinary action up to and including dismissal, termination of contract or engagement, recovery of losses, civil action and referral to law-enforcement or regulatory authorities where appropriate.

Records and Evidence

Evidence category	Examples
Governance	Approved Policy; Board or management minutes; delegated authority; role assignments
Risk assessment	Risk register; workshop evidence; annual review; action tracker; approvals
Controls	Payment approvals; call-back records; reconciliations; due diligence; access reviews; exception reports
Training	Learning-system reports; attendance; induction checklists; briefings and issued alerts
Monitoring and assurance	Audit reports; sample checks; management dashboards; action closure evidence
Incidents	Initial report; decision log; investigation record; preserved evidence; notifications; lessons learned

Review

This Policy will be reviewed at least annually and sooner where necessary to reflect relevant legislative change, Group requirements, significant business change, material control weakness or a fraud incident. Approved changes will be communicated and reflected in related procedures, training and risk assessments.

Approved by: Tamas Kaltenbacher
Tamas Kaltenbacher (Sep 29, 2026 11:03:30 GMT+1) **Date: 20/08/2026**

Tamas Kaltenbacher, BSL Managing Director