FORTISYM LIMITED

Anti-Bribery, Corruption & Business Ethics Policy

Covering the UK Bribery Act 2010, the US Foreign Corrupt Practices Act 1977 (FCPA), French Law No. 2016-1691 (Sapin II), the Modern Slavery Act 2015 and related business conduct

Document control

Document	Anti-Bribery, Corruption & Business Ethics Policy
Company	FORTISYM Limited, registered in England and Wales, company number 16906072
Registered office	43 Overstone Road, London W6 0AD
ICO registration	ZC094522
Version	1.0
Status	Approved
Policy owner	Mark Wharton, Director (Compliance Officer)
Approved by	Board of Directors (Mark Wharton, Peter Thomas)
Date of approval	18 November 2026
Effective date	18 November 2026
Next review	18 November 2027
Applies to	All directors, officers, employees, contractors, temporary staff and third-party representatives of FORTISYM

Version history

Version	Date	Author	Summary of changes
1.0	18 November 2026	Mark Wharton	First issue – approved by the Board

Contents

1. Policy statement and purpose
2. Scope and application
3. Legal framework
4. Roles and responsibilities
5. Prohibition of bribery and corruption
6. Facilitation payments
7. Gifts, hospitality, entertainment and travel
8. Dealing with public officials and public-sector procurement
9. Political and charitable donations
10. Conflicts of interest
11. Third parties: due diligence and contracts
12. Accurate books and records
13. Sanctions and export compliance
14. Modern slavery, forced labour and child labour
15. Speaking up (whistleblowing) and non-retaliation
16. Risk assessment
17. Training and communication
18. Accountability, breaches and discipline
19. Record keeping
20. Monitoring and review

1. Policy statement and purpose

1.1 FORTISYM Limited ("FORTISYM", "we") is committed to conducting business honestly, ethically and in compliance with all applicable laws. We take a zero-tolerance approach to bribery and corruption in any form, whether involving public officials or private individuals, and whether carried out directly or through a third party.

1.2 This policy forms the core of FORTISYM's compliance and ethics programme. It sets out our rules and procedures for preventing bribery and corruption, and our expectations on gifts and hospitality, conflicts of interest, accurate records, sanctions, modern slavery and speaking up.

1.3 It is designed to constitute "adequate procedures" under section 7 of the UK Bribery Act 2010, following the six principles in the Ministry of Justice guidance: proportionate procedures, top-level commitment, risk assessment, due diligence, communication (including training), and monitoring and review.

1.4 The directors of FORTISYM endorse this policy and will lead by example. No one will suffer any detriment for refusing to pay or accept a bribe, even if this results in FORTISYM losing business.

2. Scope and application

2.1 This policy applies to all directors, officers, employees (permanent, fixed-term or temporary), contractors, consultants and secondees of FORTISYM, wherever located (together, "staff").

2.2 It also applies to third parties who act for or on behalf of FORTISYM, including agents, resellers, distributors, referral partners, introducers, subcontractors and suppliers (together, "third-party representatives"). They must comply with this policy, or with equivalent standards, when acting for us.

2.3 Where local law or a customer or partner requirement is stricter than this policy, the stricter standard applies.

3. Legal framework

FORTISYM is a UK company that works with vendors, distributors and partners in the UK and EU. The following laws are particularly relevant:

- **UK Bribery Act 2010 –** offences of bribing, being bribed, bribing a foreign public official, and the corporate offence of failing to prevent bribery by an associated person. Individuals face up to 10 years' imprisonment and unlimited fines; companies face unlimited fines.
- **US Foreign Corrupt Practices Act (FCPA) –** prohibits bribery of foreign (non-US) officials and requires accurate books and records. It can apply to non-US companies where there is a US connection, for example US-dollar payments, US vendors or partners, or US-listed counterparties.
- **French Sapin II (Law No. 2016-1691) –** requires anti-corruption programmes from larger companies and is passed down by French and European partners to their supply chains.
- **Modern Slavery Act 2015 –** prohibits slavery, servitude, forced or compulsory labour and human trafficking.
- **Public Interest Disclosure Act 1998 –** protects workers who make protected disclosures from detriment and dismissal.
- **UK sanctions and export control law –** including the Sanctions and Anti-Money Laundering Act 2018 and the Export Control Order 2008.

4. Roles and responsibilities

4.1 The board of directors has overall responsibility for this policy and for ensuring FORTISYM's compliance programme is adequate and properly resourced.

4.2 The board has appointed Mark Wharton, Director, as Compliance Officer. The Compliance Officer is the executive-level individual responsible for compliance, with direct access to the board. He is responsible

for: maintaining and reviewing this policy; approving gifts, hospitality and donations where required; overseeing third-party due diligence; leading the annual risk assessment; arranging training; maintaining the registers in this policy; and receiving and investigating concerns. Contact: mark@fortisym.com.

4.3 Where a matter concerns the Compliance Officer personally, or he is unavailable, his responsibilities pass to Peter Thomas, Director.

4.4 James Bacon, Chief Revenue Officer, is responsible for ensuring that sales, marketing, partner and reseller activities comply with this policy, and that relevant third parties go through due diligence before engagement.

4.5 Every member of staff is responsible for reading, understanding and complying with this policy, and for raising concerns promptly.

5. Prohibition of bribery and corruption

5.1 A bribe is any financial or other advantage offered, promised, given, requested or accepted with the intention of inducing or rewarding the improper performance of a function or activity, or where accepting it would itself be improper. “Advantage” includes cash, gifts, hospitality, travel, loans, discounts, rebates, jobs or internships, favours, donations and any other benefit.

5.2 Staff and third-party representatives must not, directly or indirectly:

- offer, promise, give or authorise a bribe to any person, whether a public official or a private (commercial) party;
- request, agree to receive or accept a bribe from any person;
- bribe a foreign public official to obtain or retain business or a business advantage;
- use a third party, family member, intermediary or any other route to do any of the above;
- disguise an improper payment through inflated fees, margins, rebates, marketing funds, discounts or false invoices.

5.3 The prohibition covers commercial (private-sector) bribery in full, including improper payments or benefits to employees of vendors, distributors, partners, customers or competitors.

5.4 Staff must not threaten or retaliate against anyone who refuses to commit a bribery offence or who raises a concern under this policy.

6. Facilitation payments

6.1 Facilitation payments (sometimes called “grease” or “speed” payments) are small unofficial payments made to secure or speed up a routine action by an official, such as processing a visa, permit or customs clearance. They are illegal under the UK Bribery Act and are prohibited by FORTISYM in all circumstances and in all countries, even where they may be tolerated locally or permitted by other laws.

6.2 The only exception is where a person faces an imminent threat to their life, liberty or physical safety. Such a payment must be reported to the Compliance Officer as soon as possible, and recorded accurately.

7. Gifts, hospitality, entertainment and travel

7.1 Reasonable and proportionate gifts and hospitality can be a legitimate part of building business relationships. They must never be offered or accepted to improperly influence a business decision, and must never create the appearance of doing so.

7.2 All gifts and hospitality, whether given or received, must:

- be given or received openly, in FORTISYM’s name, not personally or in secret;
- be reasonable in value, appropriate to the occasion and consistent with local custom;

- not be given during, or shortly before, a tender, contract negotiation, renewal or award decision involving the recipient;
- not be in the form of cash or cash equivalents (gift cards, vouchers, prepaid cards, loans, securities or cryptocurrency) – this is prohibited in all circumstances;
- be permitted under the recipient's own rules (many vendors, distributors and public bodies have their own limits);
- be recorded accurately in the Gifts & Hospitality register (Appendix A) where required by the table below.

7.3 The following thresholds and approvals apply:

Category	Commercial (private-sector) counterparties	Public officials (see section 8)
Cash or cash equivalents	Prohibited – never permitted	Prohibited – never permitted
Gifts (given or received)	Up to £50 per item: permitted, record in register. Above £50 per item, or more than £150 to/from the same person in 12 months: prior written approval of the Compliance Officer.	Nil threshold. Any gift requires prior written approval of the Compliance Officer and must be recorded.
Hospitality and entertainment (meals, events)	Up to £100 per person per occasion: permitted if business-related and the host attends; record in register. Above £100 per person: prior written approval of the Compliance Officer.	Nil threshold. Any hospitality requires prior written approval of the Compliance Officer and must be recorded.
Travel and accommodation	Paying for a third party's travel or accommodation always requires prior written approval of the Compliance Officer. Accepting vendor-funded travel (e.g. partner events, training) requires prior written approval.	Not permitted except with prior written approval of the Compliance Officer, and only where lawful, directly connected to a legitimate business purpose and paid directly to the provider.
Promotional items (branded pens, notebooks etc. of nominal value)	Permitted; no record required.	Permitted if of nominal value (under £10) and allowed by the official's rules.

7.4 Gifts or hospitality offered to a family member or companion of a counterparty count as given to the counterparty.

7.5 If a gift cannot be refused without causing offence, it may be accepted on behalf of FORTISYM, recorded and passed to the Compliance Officer, who will decide whether it is returned, shared, raffled or donated to charity.

7.6 Vendor and distributor incentive schemes (for example sales incentive payments or prizes paid to individual staff) may be accepted only where they are disclosed to and approved in writing by the Compliance Officer, and properly accounted for.

8. Dealing with public officials and public-sector procurement

8.1 A "public official" includes anyone who holds a legislative, administrative or judicial position; anyone employed by or acting for a government, government department or agency, local authority, public body or state-owned or state-controlled enterprise (including public health, education and emergency services bodies); officials of public international organisations; political parties, party officials and candidates; and members of royal families. Employees of public-sector customers are treated as public officials under this policy.

8.2 FORTISYM participates in some public-sector tenders. When doing so, staff must:

- comply fully with the procurement rules and the instructions of the contracting authority, including any communication blackout or "standstill" periods;
- not seek or use confidential or inside information about a tender, other bidders' pricing or evaluation;
- not offer any gift, hospitality, employment or other advantage to anyone involved in the procurement;

- not collude with other bidders on pricing or bidding (bid-rigging);
- declare any conflict of interest, including any former employment relationship with the contracting authority;
- make complete and truthful declarations in tender submissions, including on exclusion grounds.

8.3 Any proposal to hire, engage or offer work experience to a current or recent (within the last 2 years) public official, or a close relative of one, who has been involved with FORTISYM's business requires prior written approval of the Compliance Officer.

9. Political and charitable donations

9.1 FORTISYM does not make political donations or contributions, in cash or in kind, to any political party, party official, candidate or campaign, in any country. Staff may take part in political activity in a personal capacity, in their own time and at their own expense, but must not suggest they act for FORTISYM.

9.2 Charitable donations and sponsorships made by or on behalf of FORTISYM must be: made to a registered or otherwise legitimate charity; lawful and ethical; not offered to influence any business decision, nor made at the request of a public official or counterparty in connection with business; approved in advance by the Compliance Officer (or, for donations he proposes, by another director); and recorded in the Gifts & Hospitality register with the recipient, amount, purpose and approver.

10. Conflicts of interest

10.1 A conflict of interest arises where a person's personal, financial or family interests, or outside activities, could influence, or appear to influence, their judgement on behalf of FORTISYM.

10.2 Staff must avoid conflicts where possible and must declare any actual or potential conflict in writing to the Compliance Officer as soon as they become aware of it. Examples include: a financial interest in a vendor, distributor, partner, supplier, customer or competitor; a close relationship with someone at such an organisation who is involved in dealings with FORTISYM; outside employment or directorships; and referral fees or personal benefits from third parties.

10.3 The Compliance Officer will record declared conflicts and agree how they are managed (for example, removing the person from the decision). Conflicts involving a director are declared to the board and handled in line with the Companies Act 2006 duties on conflicts of interest.

11. Third parties: due diligence and contracts

11.1 FORTISYM can be liable for bribes paid by third parties acting on its behalf. We therefore carry out risk-based due diligence before engaging, and periodically during the relationship with, agents, resellers, distributors, referral partners, introducers, subcontractors, consultants and suppliers.

11.2 Due diligence follows the checklist in Appendix B and covers, as a minimum: identity and company registration; ownership and control; sanctions and politically exposed person (PEP) screening; reputation and adverse media; the business rationale for the engagement; and whether fees, commissions, margins and rebates are in line with fair market value for legitimate services.

11.3 Enhanced due diligence and Compliance Officer approval are required where a third party will interact with public officials on our behalf, is paid by success fee or commission, is based in a higher-risk jurisdiction, requests unusual payment terms, or where any red flag is identified.

11.4 Contracts with third-party representatives must include an anti-bribery clause requiring compliance with the UK Bribery Act 2010 and other applicable anti-corruption laws (and this policy or equivalent standards), with rights to audit where proportionate and to terminate for breach. A model clause is set out in Appendix B.

11.5 Due diligence is refreshed at least every 2 years, or sooner on a change of ownership, scope or risk, or if a red flag arises.

11.6 Red flags that must be reported to the Compliance Officer include: requests for cash or payment to a third country or a different entity; unusually high commission or margin; requests for unexplained "extra" fees; refusal to sign anti-bribery terms; close links to a public official; and vague or missing invoices.

12. Accurate books and records

12.1 FORTISYM keeps accurate, complete and timely books, records and accounts that fairly reflect all transactions, including all gifts, hospitality, commissions, rebates, discounts, marketing development funds and payments to third parties.

12.2 No off-book or unrecorded accounts, funds or assets may be created or maintained for any purpose. No false, misleading or artificial entries may be made, and no payment may be made on the understanding that any part of it will be used for a purpose other than that described in the supporting documents.

12.3 All payments must be supported by appropriate documentation, made by traceable means (no cash payments to third parties), paid to the contracted entity in its country of business, and approved in line with FORTISYM's financial authorisations. Expense claims must be accurate and supported by receipts.

13. Sanctions and export compliance

13.1 FORTISYM complies with UK sanctions and export control law, and with other applicable regimes (including EU and, where relevant, US sanctions and export controls).

13.2 We will not deal directly or indirectly with persons, entities or countries subject to applicable sanctions, and we screen new customers, partners and suppliers against the UK sanctions list (and other relevant lists) as part of due diligence.

13.3 Some cyber security products and technologies may be subject to export controls. Staff must check vendor export classifications and obtain any required licence before supplying products or technical services across borders, and must raise any doubt with the Compliance Officer before proceeding.

14. Modern slavery, forced labour and child labour

14.1 FORTISYM has zero tolerance for slavery, servitude, forced or compulsory labour, human trafficking and illegal child labour, in our own business and our supply chains.

14.2 FORTISYM's turnover is below the £36 million threshold in section 54 of the Modern Slavery Act 2015, so we are not legally required to publish a slavery and human trafficking statement. This section is a voluntary statement of our commitments.

14.3 We commit to: paying at least the National Minimum or Living Wage as applicable; checking right to work for all staff; never retaining identity documents or charging recruitment fees to workers; not employing anyone below the minimum legal working age; considering modern slavery risk in supplier due diligence (Appendix B); and expecting our suppliers, vendors and partners to uphold equivalent standards.

14.4 Staff who suspect modern slavery or human trafficking in our business or supply chain must report it under section 15. Where there is an immediate risk to someone, contact the police (999) or the Modern Slavery & Exploitation Helpline.

15. Speaking up (whistleblowing) and non-retaliation

15.1 Anyone who suspects or becomes aware of bribery, corruption, a breach of this policy or other wrongdoing must report it as soon as possible. Staff should also report any request or offer of a bribe, even if refused.

15.2 Concerns should be raised with the Compliance Officer, Mark Wharton, at mark@fortisym.com. If the concern involves Mark Wharton, or the person does not feel able to report to him, it should be raised with Peter Thomas, Director. Concerns can be raised verbally or in writing. Third parties may use the same channels.

15.3 Concerns can also be raised confidentially. We will protect the identity of the person raising the concern as far as possible, consistent with a fair investigation and our legal obligations. Anonymous reports will be considered, although they may be harder to investigate.

15.4 All concerns will be acknowledged, assessed and investigated promptly and fairly by a person independent of the matter. The person raising the concern will be told the outcome where appropriate.

15.5 FORTISYM will not tolerate any retaliation, victimisation or detriment (including dismissal, disciplinary action, threats or unfavourable treatment) against anyone who raises a concern in good faith or refuses to take part in bribery, even if the concern turns out to be mistaken. Workers who make protected disclosures are protected under the Public Interest Disclosure Act 1998. Anyone who retaliates will face disciplinary action.

15.6 Staff may also seek independent advice from the charity Protect (protect-advice.org.uk) or report to an appropriate prescribed person or regulator, such as the Serious Fraud Office.

16. Risk assessment

16.1 The Compliance Officer will lead a documented anti-corruption risk assessment at least annually, and also when FORTISYM enters a new market, sector, partner model or significant tender, or following an incident.

16.2 The assessment considers country, sector, transaction, business opportunity and business partnership risks, rates each risk by likelihood and impact, records existing controls and agrees further actions with owners and dates. It is reported to the board.

16.3 The initial assessment is set out in Appendix C.

17. Training and communication

17.1 All staff receive this policy and anti-corruption and ethics training on joining FORTISYM (within their first month) and must sign the acknowledgement at Appendix E.

17.2 Refresher training, including anti-corruption, gifts and hospitality, third-party risk and speaking up, is delivered at least annually to all staff and in particular to Senior Management, Sales & Marketing, Finance and Procurement roles. Additional targeted training is given where the risk assessment identifies a need.

17.3 Training completion is recorded in the training log (Appendix D) and retained.

17.4 This policy is communicated to third-party representatives at the start of the relationship, and our zero-tolerance approach is stated in relevant contracts and partner onboarding.

18. Accountability, breaches and discipline

18.1 Compliance with this policy is a condition of employment and engagement. Each member of staff must sign the acknowledgement form at Appendix E on joining and on each material update of the policy.

18.2 Any breach of this policy by staff will be treated as a disciplinary matter and may result in sanctions up to and including summary dismissal for gross misconduct. Contractors and consultants in breach may have their engagement terminated immediately.

18.3 Breaches by third-party representatives may result in suspension of payments and immediate termination of the contract, and FORTISYM may seek to recover losses.

18.4 Where appropriate, FORTISYM may report suspected offences to the relevant authorities and will cooperate with any investigation.

19. Record keeping

FORTISYM keeps the following records for at least 6 years: the Gifts & Hospitality register and approvals; due diligence files; conflict of interest declarations; risk assessments; training records; signed acknowledgements; donation records; and records of concerns raised and investigations. Personal data in these records is processed in line with UK data protection law and FORTISYM's data protection arrangements (ICO registration ZC094522).

20. Monitoring and review

20.1 The Compliance Officer monitors compliance with this policy, including periodic review of the Gifts & Hospitality register, expense claims, third-party payments and due diligence files.

20.2 The policy is reviewed by the board at least annually, and earlier if there is a material change in the law, in FORTISYM's business or risk profile, or following an incident. The review considers the risk assessment, training completion, concerns raised and any lessons learned.

20.3 Questions about this policy should be directed to the Compliance Officer at mark@fortisym.com.

Operational appendices (the gifts and hospitality register, due diligence checklist, risk assessment, training log, acknowledgement form and board minute) are maintained internally and are not published with this public version of the policy.