

WHISTLEBLOWING AND REPORTING CONCERNS POLICY

Internal and External Reporting

Document ID	P-23	Issue date	01/01/2026
Version	1	Status	Signed Off



REPORT A CONCERN - ANONYMOUS ONLINE FORM

[Open the 2012 Security Anonymous Report a Concern Form](#)

The form is available to employees and external parties. A name or contact details are not required. Contact details may be supplied voluntarily if you want a confidential response.

URGENT RISK: Do not use the online form for an emergency or an incident requiring an immediate operational response. Call 999 where there is immediate danger, or contact the 2012 Security Control Room for urgent operational matters.

1. PURPOSE, SCOPE AND STATUS

1.1 2012 Security Ltd encourages concerns about serious wrongdoing to be raised at the earliest opportunity. This policy provides safe routes for reporting concerns connected with the Company, its workforce, services, client assignments, subcontractors or supply chain.

1.2 This policy is intended for internal use and external publication. It applies to employees, workers, agency workers, officers, job applicants, contractors, subcontractors, suppliers, clients, customers and any other person who has information about wrongdoing connected with 2012 Security Ltd.

1.3 The Company will assess genuine concerns under this policy even where the reporter does not have statutory whistleblowing status. Statutory protection depends on the reporter's legal status, the nature of the disclosure and the route used.

1.4 The statutory summary in this policy relates to Great Britain. Different whistleblowing legislation applies in Northern Ireland.

2. WHAT WHISTLEBLOWING MEANS

2.1 Whistleblowing is the reporting of information about wrongdoing where the reporter reasonably believes the disclosure is in the public interest.

2.2 For workers, a disclosure may qualify for statutory protection where the worker reasonably believes that the information tends to show that one or more of the following has occurred, is occurring or is likely to occur:

- a criminal offence, including fraud, theft, bribery or corruption;
- a failure to comply with a legal obligation;
- a miscarriage of justice;
- danger to the health or safety of any person;
- damage to the environment;
- sexual harassment; or
- the deliberate concealment of information tending to show any of the above.

2.3 Sexual harassment has been an express category of qualifying whistleblowing disclosure in Great Britain since 6 April 2026.

2.4 The reporter does not need to prove the wrongdoing. The legal test concerns reasonable belief, public interest and the route by which a disclosure is made. A disclosure can concern past, current or likely future wrongdoing, including conduct occurring outside the UK where relevant.

3. SERIOUS CONCERNS COVERED BY THIS POLICY

3.1 In addition to the statutory categories above, the Company encourages reports about serious ethical, operational, regulatory or compliance concerns connected with its activities, including:

- modern slavery, human trafficking, forced labour, debt bondage or other labour exploitation;
- unlicensed security activity, misuse of an SIA licence, false ACS claims or other regulatory non-compliance;
- falsification of vetting, right-to-work, training, patrol, attendance, time, pay, payroll or compliance records;

- security failures, safeguarding concerns, client risk, concealment of incidents or deliberate circumvention of control measures;
- data protection, privacy, cyber-security or confidentiality breaches;
- undisclosed conflicts of interest, bribery, improper personal benefit, secret commissions or misuse of Company or client assets;
- unsafe working practices, deliberate concealment of accidents or failures to report required health and safety information;
- serious financial irregularity, tax evasion facilitation, false invoicing or deliberate manipulation of Company records; and
- retaliation, victimisation, attempts to identify an anonymous reporter, or attempts to pressure or silence a person who has raised or assisted with a concern.

3.2 A concern that is solely about the reporter's own employment, pay, treatment or contractual position will usually be dealt with under the grievance, complaints or contractual procedure. A personal complaint may also contain a whistleblowing disclosure where it raises a wider public-interest concern.

WHISTLEBLOWING OR GRIEVANCE?

A grievance is normally a personal employment complaint. Whistleblowing concerns wrongdoing with a wider public-interest element. A report can contain both. Managers must not reject a disclosure merely because it also contains a personal complaint.

4. HOW TO REPORT A CONCERN

4.1 A concern may be raised through any of the following routes:

- a supervisor, line manager or Director;
- the HR team at 2012hr@2012security.co.uk;
- the public Anonymous Report a Concern Form, available by QR code or link in this policy; or
- an appropriate external authority, prescribed person, law-enforcement body or independent adviser, as described in section 11.

4.2 A reporter may use any route they reasonably consider appropriate. They do not have to report through the person who is the subject of the concern or through a reporting line that creates a conflict.

4.3 Where the concern involves a manager, Director, HR representative or anyone who would normally receive or handle the report, the reporter should use an alternative route and identify the conflict. The implicated person must not control the assessment, evidence, investigation or outcome.

4.4 Where no suitably independent internal decision-maker is available, the Company will appoint an external investigator, legal adviser, HR adviser or other competent independent person. This does not prevent the reporter from using an appropriate external reporting route.

4.5 A concern may be raised verbally or in writing. A reporter who raises a concern verbally may be asked to confirm the key facts so that an accurate record can be maintained.

5. OPEN, CONFIDENTIAL AND ANONYMOUS REPORTING

5.1 Reports may be made openly, confidentially or anonymously:

- Open - the reporter identifies themselves and agrees that identity may be shared where reasonably necessary to deal with the concern.
- Confidential - authorised personnel know the reporter's identity but will protect it and disclose it only where necessary or required by law.
- Anonymous - the reporter does not provide their identity. The online form does not require a name or contact details.

5.2 External stakeholders may use the same anonymous form and may leave all identifying and contact fields blank. A reporter who wants to reduce the possibility of identification through workplace systems may choose to use a personal device and connection.

5.3 Anonymous reporting may limit the Company's ability to ask follow-up questions, test evidence or provide an outcome. Reporters may use the optional reference word or phrase in the form when submitting further information.

5.4 The Company cannot guarantee that identity will never be inferred from facts, location, timing, documents or circumstances. It will not deliberately seek to identify an anonymous reporter unless there is a lawful, necessary and proportionate reason to do so.

6. INFORMATION TO PROVIDE AND EVIDENCE

6.1 A report should include as much of the following information as the reporter knows:

- what happened, is happening or is expected to happen;
- when and where it happened;

- the people, organisations, clients, suppliers or sites involved;
- whether anyone is at immediate risk;
- whether the concern is continuing or has already been reported;
- the reason the reporter considers the matter serious or in the public interest; and
- any documents, messages, photographs, witnesses, system records or other evidence which may already exist.

6.2 The reporter is not expected to prove the allegation or conduct an investigation. No one should obtain evidence unlawfully, access systems without authority, secretly remove protected information without justification, interfere with evidence, confront the subject of the report, or place themselves or another person at risk.

6.3 Once a concern has been raised, relevant records must not be deleted, altered, overwritten or destroyed. Where necessary, the Company will issue instructions to preserve CCTV, email, access-control records, payroll data, messages, personnel records, telematics, client records or other relevant evidence.

7. RESPONSIBILITIES OF MANAGERS AND RECIPIENTS

7.1 Any manager, supervisor, Director or other person who receives a concern must treat it seriously, protect confidentiality and escalate it promptly to an authorised person unless they are themselves formally assigned to handle the matter.

7.2 A recipient must not:

- dismiss the concern as a grievance without considering whether it contains a public-interest disclosure;
- promise absolute confidentiality or promise a particular outcome;
- warn, coach or confront the person accused where doing so could compromise safety, evidence or a fair investigation;
- conduct an informal investigation outside their authority;
- attempt to identify an anonymous reporter; or
- allow the reporter to suffer retaliation, loss of work or other disadvantage because a concern was raised.

7.3 Immediate risks involving safety, safeguarding, crime, data loss, regulatory exposure or evidence destruction must be escalated without delay. Emergency services must be contacted first where there is immediate danger.

8. ASSESSMENT AND INVESTIGATION

8.1 Reports will be assessed as soon as reasonably practicable by authorised personnel. The initial assessment will consider immediate safety, safeguarding, security, regulatory, client, financial, data-protection, conflict-of-interest and evidence-preservation risks.

8.2 The Company will determine the appropriate route, which may include an internal investigation, external independent investigation, referral to a regulator or law-enforcement body, safeguarding action, disciplinary process, supplier review, client notification, control improvement or another proportionate response.

8.3 Where an investigation is required, it will be conducted fairly and, so far as reasonably possible, independently of the people concerned. The investigator must have appropriate competence and no material conflict of interest.

8.4 The person who is the subject of a concern is entitled to fair treatment. A report is not a finding of wrongdoing, and conclusions must be based on available evidence and a fair process.

8.5 Where contact details are available, the Company will acknowledge the report and provide appropriate updates where reasonably possible. The Company may be unable to disclose detailed findings, disciplinary action, personal data, legally privileged material or information which could prejudice legal, regulatory or criminal proceedings.

8.6 A concern raised on a genuine or reasonably held belief will not result in action against the reporter merely because it is not substantiated. Deliberately providing information known to be false, or fabricating evidence, may result in disciplinary or contractual action.

9. CONFIDENTIALITY, PROTECTION AND NON-RETALIATION

9.1 2012 Security Ltd will take reasonable steps to protect the reporter's identity and the confidentiality of the report. Information will be shared only with people who reasonably need it for assessment, investigation, legal advice, safeguarding, regulatory reporting or other legitimate action.

9.2 Absolute confidentiality cannot be guaranteed where disclosure is required by law, necessary to protect a person, essential for a fair investigation, required by a regulator or law-enforcement body, or necessary for civil or criminal proceedings.

9.3 The Company will not tolerate dismissal, loss of work, withholding of shifts, threats, bullying, harassment, intimidation, discrimination, adverse references, contractual disadvantage or any other retaliation because a person raised, supported or assisted with a genuine concern. This applies to conduct by managers, colleagues, workers, agents, contractors and others within the Company's control.

9.4 Any suspected retaliation must be reported immediately. The Company may take protective steps, including changing reporting arrangements, separating involved persons, preserving work allocation, or taking disciplinary or contractual action where appropriate.

9.5 Workers who make a qualifying protected disclosure through an appropriate route may have statutory protection from detriment and, for employees, automatic unfair dismissal. External parties who are not workers may not have the same statutory rights, but the Company's non-retaliation commitment applies to conduct within its control.

9.6 No Company confidentiality clause, non-disclosure agreement, settlement term or other contractual provision is intended to prevent a person from making a protected disclosure or another disclosure which the law provides cannot be restricted. The Company will not seek to enforce a term to the extent that doing so would be unlawful.

10. RECORDS, DATA PROTECTION AND GOVERNANCE

10.1 Whistleblowing records will be held securely with access restricted to authorised persons. Personal information will be processed only where necessary and proportionate and in accordance with applicable data-protection law and Company retention requirements.

10.2 Information may be shared with regulators, law-enforcement bodies, clients, insurers, professional advisers, investigators or other parties where lawful and reasonably necessary to address the concern.

10.3 The Company will maintain a restricted record of whistleblowing cases sufficient to show the date, subject category, risk assessment, conflict check, investigator or owner, key decisions, outcome and actions taken. Unnecessary personal information should not be recorded.

10.4 An anonymised review of themes, control failures, retaliation concerns and corrective actions will be undertaken at least annually by the appropriate Director or governance owner. Anyone implicated in a case must be excluded from oversight of that case.

11. EXTERNAL REPORTING AND INDEPENDENT ADVICE

11.1 The Company encourages concerns to be raised internally where appropriate so that they can be addressed quickly. However, a reporter is not required to approach the Company before contacting an appropriate regulator, law-enforcement body or other authorised organisation.

Private security - Security Industry Authority (SIA)

The SIA is a prescribed person for specified matters relating to the private security industry, including offences under the Private Security Industry Act 2001, whether an individual or business is fit and proper to hold a licence or approval, and conduct that may undermine the regulation of security operatives or approved providers.

[Report a crime or concern to the Security Industry Authority](#)

Modern slavery, forced labour and exploitation

Modern Slavery & Exploitation Helpline: [08000 121 700 or online reporting](#)

Gangmasters and Labour Abuse Authority (GLAA): [0800 432 0804 and reporting guidance](#)

Police: [999 in an emergency or 101 for a non-emergency](#)

Crimestoppers: [anonymous reporting on 0800 555 111](#)

Other prescribed persons and independent advice

Depending on the subject, another prescribed person may be appropriate, including the Health and Safety Executive for relevant health and safety matters, the Information Commissioner for data protection matters, or HM Revenue & Customs for tax and National Insurance matters. The current GOV.UK list should be checked before making a prescribed-person disclosure.

[GOV.UK - current list of prescribed people and bodies](#)

[Protect - independent whistleblowing advice](#)

[Acas - whistleblowing at work guidance](#)

11.2 A reporter may also seek advice from a trade union or legal adviser. Legal protection for disclosure to the media, social media or another third party is limited and depends on specific statutory conditions. Anyone considering wider public disclosure should obtain independent advice first.

12. AWARENESS, TRAINING AND REVIEW

12.1 This policy may be published on the Company website and shared with employees, agency workers, subcontractors, suppliers, clients, customers and other stakeholders. The anonymous reporting link and QR code may also be included in induction material, assignment instructions, supplier onboarding documents and workplace notices.

12.2 Managers and others who may receive concerns must be briefed on this policy, including confidentiality, conflict checking, evidence preservation, non-retaliation and the need to escalate serious concerns promptly.

12.3 This policy will be reviewed at least annually and whenever there is a material change in law, regulatory guidance, reporting arrangements, Company structure or following a serious whistleblowing case or identified control failure.

13. LEGAL AND OPERATIONAL REFERENCES

13.1 This policy has been reviewed with reference to the following legislation and official guidance current at 8 August 2026:

- Employment Rights Act 1996, Part IVA - protected disclosures;
- Public Interest Disclosure Act 1998;
- Employment Rights Act 2025, including the express protection of disclosures relating to sexual harassment from 6 April 2026 and restrictions affecting confidentiality provisions concerning harassment and discrimination;
- Public Interest Disclosure (Prescribed Persons) Order 2014, as amended;
- Equality Act 2010, including the statutory meaning of sexual harassment;
- Data Protection Act 2018 and UK GDPR;
- Private Security Industry Act 2001 and Security Industry Authority reporting guidance;
- GOV.UK whistleblowing guidance for employers and current list of prescribed persons; and
- Acas guidance: Whistleblowing at work.

13.2 This policy provides operational guidance and is not a substitute for individual legal advice. Statutory protection depends on the circumstances of the disclosure and the applicable law.

14. DOCUMENT CONTROL

Document owner	AON - Ann O'Neill
Reviewer	TT - Theo Theodorou
Approver	Managing Director (MD)
Document ID	P-23
Document reference	P-23/1-01/01/26
Version	1
Previous / legacy reference	None - first controlled issue
Status	Signed Off
Effective date	01/01/2026
Revision date	1 September 2026
Review date	8 January 2027; earlier on material change

APPENDIX A - REPORTING QUICK ACTION CARD

IMMEDIATE ACTION

1. If anyone is in immediate danger, call 999.
2. Choose a reporting route that is not conflicted.
3. Give facts, dates, people, sites and known evidence.
4. Do not investigate, confront the subject or obtain evidence unlawfully.
5. Preserve relevant records and report any retaliation immediately.

A1. WHAT TO REPORT

- criminal or fraudulent conduct;
- health and safety danger;
- sexual harassment with a public-interest element;
- SIA licensing, ACS or regulatory wrongdoing;
- modern slavery or labour exploitation;
- falsified vetting, RTW, attendance, pay or compliance records;
- serious security, safeguarding, data or financial failures;
- conflicts of interest, improper personal benefit or misuse of assets;
- concealment of wrongdoing; or
- retaliation against someone who has raised or supported a concern.

A2. INTERNAL ROUTES

- Supervisor, line manager or Director
- HR: 2012hr@2012security.co.uk
- Anonymous Report a Concern Form - use the QR code or link in this policy
- If the normal recipient is implicated, use an alternative route and identify the conflict

A3. KEY PROTECTIONS

- You do not need to prove the allegation.
- A genuine concern is not misconduct merely because it is not substantiated.
- The Company will protect confidentiality as far as reasonably possible.
- Retaliation, loss of shifts, threats, bullying or disadvantage because of a genuine concern are prohibited.
- A conflicted or implicated person must not control the investigation.

A4. EXTERNAL ROUTES

Appropriate external routes may include the SIA, HSE, ICO, HMRC, police, GLAA or another prescribed person or regulator depending on the subject. Independent advice is available from Protect, Acas, a trade union or legal adviser.

A5. DO NOT

- place yourself or another person at risk;
- access systems or records without authority;
- remove or alter evidence;
- warn or confront the person accused;
- post allegations on social media as a substitute for a proper reporting route; or
- attempt to identify an anonymous reporter.

Administrative Approval authority is not a record of signature. Previous substantive review date retained.