The Steadfast Security Group

Whistleblowing Policy

1 Hackworth Road,
Northwest Industrial Estate
Peterlee
County Durham
SR8 2JQ

Tel: 0191 518 0837
Email: contact@steadfastsecurity.co.uk
Web: www.steadfastsecurity.co.uk

SSG.I.0066

GENERAL INFORMATION			
Organisation:	**Steadfast Security Group**		
Version:	**02**	Document Owner:	**Compliance Manager**
Issue Date:	**20 November 2025**	Next Review:	**20 November 2028**
Email Address:	**Steven.hope@steadfastsecurity.co.uk**	Tel Number:	**0191 518 0837**

AMENDMENTS				
Ser No	**Section**	**Reason for Amendment**	**Amended By**	**Date**

REVIEWS				
Ser No	**Date**	**Reason for Review**	**Reviewed By**	**Next Review**

SCOPE

1. Steadfast Security Group, which includes Steadfast Security Solutions Ltd, Steadfast Security Systems Ltd, Steadfast Secure Storage Ltd, and Complete Security (Europe) Ltd, is committed to promoting transparency and integrity throughout our operations. This policy sets out the rights of staff members to make qualified and protected disclosures, commonly referred to as whistleblowing, and ensures that concerns about wrongdoing can be raised safely and responsibly. We expect all staff to maintain high standards of conduct, but we acknowledge that issues can arise from time to time. A culture of openness and accountability is essential to prevent illegal or unethical practices and to address them promptly when they occur.

2. All staff members should feel confident to report suspected wrongdoing, knowing that their concerns will be taken seriously and investigated appropriately. Genuine disclosures will be protected, and individuals will not face reprisals for raising concerns, even if they are mistaken. Any questions regarding this policy should be directed to the HR Manager in the first instance. This policy explains the legal framework for whistleblowing and provides guidance on how to raise concerns about malpractice or wrongdoing.

3. The policy applies to all individuals working for Steadfast Security Group in the UK, at all levels, including senior managers, officers, employees, consultants, trainees, homeworkers, part-time and fixed-term workers, casual workers, agency workers, volunteers, and interns. It is not intended for complaints about personal employment circumstances, such as treatment at work. Such matters should be addressed through the Steadfast Security Group Grievance Procedure. This policy does not form part of any employment contract and may be amended at the employer's discretion at any time.

KEY LEGISLATION

4. **Public Interest Disclosure Act 1998 (PIDA):** PIDA is the cornerstone of UK whistleblowing law. It protects workers from dismissal or detrimental treatment for making a "protected disclosure" in the public interest. A qualifying disclosure must reasonably show wrongdoing such as a criminal offence, breach of legal obligation, miscarriage of justice, health and safety risks, environmental damage, or deliberate concealment of any of these. Protection applies from day one of employment and covers employees, agency workers, trainees, and certain contractors. Dismissal for whistleblowing is automatically unfair, and there is no cap on compensation.

5. **Employment Rights Act 1996 (as amended by PIDA):** This Act incorporates whistleblowing protections into employment law. It makes it unlawful to dismiss or subject a worker to detriment because they made a protected disclosure. It also sets out the criteria for qualifying disclosures and provides the right to bring claims before an employment tribunal.

6. **UK GDPR and Data Protection Act 2018:** Whistleblowing often involves processing personal data about the whistleblower, alleged wrongdoers, and witnesses. Organisations must comply with UK GDPR principles, including lawfulness, fairness, transparency, data minimisation, and security. Special category data or criminal offence data may require additional safeguards. Confidentiality and secure handling of reports are essential to avoid breaches.

7. **Worker Protection Act 2024:** Although primarily aimed at preventing workplace harassment, this Act reinforces the need for robust whistleblowing policies. Employers must take reasonable steps to prevent harassment and ensure employees can report concerns, including discrimination or harassment, without fear of retaliation.

8. **Surveillance Camera Code of Practice:** For organisations using CCTV, the Code requires compliance with data protection and privacy standards. Whistleblowing policies should align with these principles when concerns relate to misuse of surveillance systems or breaches of privacy

ROLES AND RESPONSIBILITIES

9. **The Board of Directors** holds ultimate responsibility for ensuring that the organisation operates with integrity and transparency. They must approve and periodically review the whistleblowing policy, allocate sufficient resources for its implementation, and oversee that reported concerns are addressed promptly and effectively. Their role includes setting the tone for an open culture where ethical behaviour is prioritised.

10. **The Chief Compliance Officer** is responsible for managing the whistleblowing framework and ensuring compliance with all relevant legislation. This includes monitoring the effectiveness of the policy, overseeing investigations to ensure fairness and confidentiality, and reporting findings to the Board. The Chief Compliance Officer also ensures that staff are aware of their rights and obligations under the policy.

11. **The HR Manager** acts as the first point of contact for whistleblowing queries and concerns. They are responsible for guiding employees through the reporting process, ensuring confidentiality, and supporting investigations. The HR Manager must also ensure that whistleblowers are protected from retaliation and that appropriate records are maintained in line with data protection requirements.

12. **Management** plays a critical role in creating a culture of openness and accountability. Managers must encourage staff to raise concerns without fear, ensure that any issues reported are escalated promptly, and cooperate fully with investigations. They are also responsible for reinforcing policy awareness within their teams and addressing any operational risks identified through whistleblowing.

13. **Employees** have a duty to uphold the organisation's standards of integrity and report any suspected wrongdoing in good faith. They should follow the procedures outlined in the whistleblowing policy and cooperate with investigations when required. Employees are also expected to maintain confidentiality and avoid victimising colleagues who raise concerns.

14. **Visitors and Contractors** are expected to comply with the organisation's ethical standards while on site or engaged in work for the company. They should report any concerns they observe through the appropriate channels and cooperate with investigations if necessary. Their adherence to these principles helps maintain integrity across all operations.

TYPES OF CONCERNS

15. **Whistleblowing** refers to the disclosure of information about suspected wrongdoing or risks in the workplace, as defined by the *Public Interest Disclosure Act 1998* (the "Act"). For a disclosure to qualify as whistleblowing, it must meet the criteria of a *Qualifying Disclosure* under the Act. This means the staff member must reasonably believe that the disclosure is in the public interest; and the wrongdoing is occurring, has occurred, or is likely to occur.

16. Examples of such disclosures include:

- Criminal offences
- Miscarriages of justice
- Risks to health and safety
- Environmental damage
- Breach of legal obligations
- Bribery
- Financial fraud or mismanagement
- Breaches of Steadfast Security Group's internal policies, including Codes of Conduct
- Unauthorised disclosure of confidential information
- Deliberate concealment of any of the above

17. A whistleblower is any employee or worker who raises a genuine concern about suspected wrongdoing or risks affecting Steadfast Security Group's activities, as outlined in this Policy. Such concerns should be reported through the procedures set out in the Policy. If you are unsure whether your concern falls within its scope, please seek advice from the HR Manager.

HOW TO RAISE A CONCERN

18. To make a whistleblowing disclosure that qualifies as a *Protected Disclosure* under the law, it must be raised correctly by following the steps in this Policy.

a. Ensure your disclosure qualifies as a **Protected Disclosure** by following the steps in this Policy.

b. **First point of contact:** Raise your concern with the **HR Manager**, either in person or in writing. The HR Manager will:

- Discuss the issue with you.
- Attempt to resolve it promptly.
- Refer it to the appropriate department if necessary.

c. If the matter is **serious**, **not addressed**, or you **prefer not to approach HR**, contact the relevant person:

- **Compliance Manager** – for concerns about dishonesty, fraud, or corruption.
- **Health and Safety Manager** – for health and safety issues.

WIDER DISCLOSURES

19. This Policy is designed to provide an internal process for reporting, investigating, and addressing workplace wrongdoing. In most cases, concerns should be raised internally within Steadfast Security Group. However, the law recognises that in certain circumstances it may be appropriate to report concerns to an external body, such as a regulator. Reporting to the media is almost never appropriate, and we strongly advise seeking guidance, such as legal advice, before making any external disclosure.

20. Specific rules apply when making a Protected Disclosure to an external party. For example, you must reasonably believe the information is substantially true, act without personal gain, and consider whether it is reasonable to disclose in the circumstances. For further guidance, please contact the HR Manager.

WHAT TO EXPECT FROM STEADFAST

21. Once a concern is raised, it will be assessed to determine the appropriate action or investigation. You will be informed who is handling the matter, how to contact them, and whether further information or assistance is required. You may be asked to attend additional meetings to provide details, and you are entitled to bring a colleague or union representative, who must maintain confidentiality.

22. All allegations will be investigated thoroughly, and while we aim to keep you updated on progress and timescales, confidentiality may limit the details we can share about the investigation, its outcome, or any disciplinary action. Any information provided should be treated as confidential.

23. If it is found that a concern was raised maliciously or for personal gain, disciplinary action may be taken under our Disciplinary Procedure. While we cannot guarantee the outcome you seek, we will always handle your concerns fairly and appropriately.

ASSURANCES

24. Steadfast Security Group is committed to ensuring that all staff can raise concerns openly under this Policy. If you are worried about reprisals for reporting a concern, additional measures can be taken to protect your confidentiality.

25. Under whistleblowing law, employees and workers must not suffer any detrimental treatment for raising a concern, even if the concern proves to be mistaken. Detrimental treatment includes dismissal, disciplinary action, threats, or any other unfavourable treatment linked to whistleblowing. We will take all reasonable steps to prevent this. If you believe you have experienced such treatment, inform the HR Manager immediately. If the issue is not resolved, you may escalate it through the Grievance Procedure.

26. Managers and staff must never threaten or retaliate against anyone who raises a whistleblowing concern. Any such behaviour will result in disciplinary action.

PROTECTION FROM VICTIMISATION

27. Whistleblowers are entitled to full protection from any form of victimisation, retaliation, or adverse treatment because of raising a concern under this Policy. This includes, but is not limited to, harassment, intimidation, threats, discrimination, or any action that could negatively impact their employment, career progression, or working environment. Steadfast Security Group takes these protections seriously and will enforce them rigorously.

28. Any individual, regardless of position, who engages in victimisation or retaliatory behaviour against a whistleblower will face formal disciplinary action. Such action may include warnings, suspension, or, in serious cases, termination of employment. These measures are in place to ensure that all staff feel safe and supported when reporting wrongdoing and that the integrity of the whistleblowing process is maintained.

FEEDBACK

29. Steadfast encourages all employees to share feedback on its policies to support continuous improvement. If you have any comments, questions, or concerns regarding this policy, please contact the Compliance Manager by emailing steven.hope@steadfastsecurity.co.uk. Your input is valued and helps ensure our policies remain clear, effective, and inclusive.

APPROVAL

30. This policy has been formally approved by the Board of Directors of Steadfast Security Group and is authorised for distribution across the organisation. All employees are expected to familiarise themselves with its contents and adhere to the principles and procedures outlined herein.

Paul Harbord
Managing Director, The Steadfast Security Group
20 November 2025