



Enterprise security solutions that deliver more than just security

**Document Title** Whistleblowing Policy

**Date of Issue** 09/10/2026

**Issue Number** 2026-v2.0

**Classification** Internal

**Approval** Richard Parnell – Chief Executive Officer

**Signature**

| Document Issue | Date of Issue | Changes from previous version                                                                                      |
|----------------|---------------|--------------------------------------------------------------------------------------------------------------------|
| 2026-v2.0      | 09/10/2026    | Updated the policy document number and formatting and revised the content to include dedicated reporting channels. |
|                |               |                                                                                                                    |

## Total Security Protection Ltd.

**Head Office:** Watford

**Other Offices:** Leeds | Dublin | Frankfurt | Hong Kong | Portugal

**T:** +44 (0) 1923 22 88 66 | **E:** sales@tsp.co.uk | **W:** www.tsp.co.uk

Registered in England & Wales no. 2330115

Registered Office: 4 Century Court, Tolpits Lane, Watford, Herts WD18 9RS



Cert No. 21176  
ISO 9001  
ISO 14001  
ISO 27001  
ISO 45001



|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

**Contents**

**1.0 Whistleblowing Policy .....3**

1.1 Purpose.....3

1.2 Scope .....3

1.3 Qualifying Disclosure .....3

**2.0 Raising a Concern.....4**

2.1 Internal Reporting.....4

2.2 Dedicated Email Channel.....4

2.3 Dedicated Telephone Channel.....4

2.4 Information to Include.....5

**3.0 Handling and Investigation of Concerns .....5**

**4.0 Confidentiality and Anonymous Reporting .....6**

**5.0 Protection from Detrimental Treatment .....7**

**6.0 Data Protection and Record Keeping.....7**

**7.0 External Disclosures .....8**

**8.0 Responsibilities .....9**

8.1 Employees, Contract Workers and Other Reporting Individuals .....9

8.2 HR Team .....9

8.3 Directors and Senior Management .....9

8.4 Compliance Team .....10

8.5 IT Team.....10

**9.0 Policy Review.....10**

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

## 1.0 Whistleblowing Policy

### 1.1 Purpose

Total Security Protection Ltd, its subsidiaries, and affiliated companies (referred to in this Policy as "the Company"), are committed to conducting business ethically, responsibly and in compliance with applicable legal and regulatory requirements.

This Policy establishes the arrangements for reporting, assessing and managing concerns about suspected wrongdoing and seeks to ensure that individuals can raise concerns without fear of retaliation.

### 1.2 Scope

This Policy applies to employees, workers, agency workers, contractors, consultants and other individuals carrying out work for or on behalf of the Company. The Company's whistleblowing reporting channels are also available to suppliers, customers and other interested parties who wish to raise concerns relating to the Company's activities.

Concerns may be raised through the Company's management structure or through the whistleblowing reporting channels described in this Policy.

The statutory protections available under whistleblowing legislation depend on the individual circumstances of the disclosure and whether it qualifies as a protected disclosure.

This Policy is not intended to address personal employment grievances that do not involve wrongdoing in the public interest. Such matters should normally be raised through the appropriate HR procedure.

### 1.3 Qualifying Disclosure

A qualifying disclosure is a disclosure of information that an individual reasonably believes is made in the public interest and tends to show that the Company, or a person acting in connection with the Company, has committed, is committing or is likely to commit a relevant failure.

A relevant failure may include:

- a. Committing a criminal offence.
- b. Failing to comply with a legal obligation.
- c. A miscarriage of justice.
- d. Endangering the health and safety of an individual.
- e. Risk of, or actual, environmental damage.
- f. Sexual harassment.
- g. Deliberate concealment of information relating to any of the above.

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

This may include concerns about fraud, bribery, corruption, data protection breaches, misuse of personal information, modern slavery, human rights abuses, or other suspected wrongdoing where it falls within one of the categories listed above.

The concern may relate to something that has happened in the past, is happening now, or is likely to happen in the future.

The Employment Rights Act 1996 protects workers who make qualifying disclosures. Workers must not be subjected to any detriment for raising a qualifying concern, and employees are protected from unfair dismissal where the disclosure is made in accordance with the law.

## 2.0 Raising a Concern

### 2.1 Internal Reporting

The Company encourages individuals to raise concerns internally in the first instance so that they can be assessed and addressed promptly.

Where appropriate, a concern may be raised with:

- The individual's Line Manager.
- The HR Team.
- A Director.
- The Chief Executive Officer.
- The dedicated whistleblowing reporting channels detailed below.

If a concern involves, or could reasonably be perceived to involve, the person who would normally receive the report, the individual should use one of the alternative reporting routes.

### 2.2 Dedicated Email Channel

Concerns may be submitted by email to:

[Whistleblowing@tsp.co.uk](mailto:Whistleblowing@tsp.co.uk)

Access to the dedicated mailbox will be restricted to authorised recipients designated by the Company.

Individuals using the email reporting channel should be aware that their email address may identify them. Anyone who wishes to report a concern anonymously should use the dedicated telephone voicemail option and avoid providing information that could reveal their identity.

### 2.3 Dedicated Telephone Channel

Concerns may be reported by calling the Company's main telephone number and selecting:

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

## Option 6 – Whistleblowing

Option 6 will direct the caller to a dedicated whistleblowing voicemail inbox. A caller may leave a report anonymously and is not required to provide their name or contact details.

The telephone message should contain sufficient information to enable the concern to be assessed and investigated where appropriate. Guidance on the information that should be provided is set out in Section 2.4.

If the concern requires urgent attention, the caller should state **"URGENT"** at the beginning of the message and provide sufficient information to explain why prompt action may be required.

### 2.4 Information to Include

Individuals raising a concern should provide as much factual information as they reasonably can. They are not expected to investigate the matter themselves or prove that wrongdoing has occurred.

Where available, a report should include:

- A clear description of the concern.
- Relevant names, dates and locations.
- How the individual became aware of the matter.
- Whether the concern has previously been reported and, if so, to whom.
- Details of any supporting documents, communications or other evidence.
- Whether there appears to be an immediate or continuing risk.

An individual should not attempt to obtain evidence unlawfully or access information they are not authorised to access.

## 3.0 Handling and Investigation of Concerns

The HR Team will monitor the dedicated whistleblowing mailbox and voicemail inbox and ensure that appropriate cover arrangements are in place during periods of absence.

On receipt of a report, the Company will:

- Record the concern securely.
- Conduct an initial assessment of the information provided.
- Consider whether urgent action is necessary.
- Determine whether the matter falls within this Policy or should be addressed under another Company procedure.
- Escalate the matter to an appropriate Director, senior manager or other authorised person where required.
- Decide whether an investigation or other action is appropriate.

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

- Identify and manage any actual or potential conflict of interest affecting those handling the report.

Where contact details have been provided, the Company will normally acknowledge receipt and may request further information.

The reporting individual may be informed about the general progress or conclusion of the matter where it is appropriate and lawful to do so. However, the Company may be unable to provide detailed information where this would breach another person's confidentiality, data protection rights or other legal obligations.

The Company will assess all reports received. An investigation may not be possible where insufficient information has been provided, particularly where the report is anonymous and there is no means of seeking clarification.

Where appropriate, the Company may appoint an internal or external person with suitable independence and competence to investigate the concern.

## 4.0 Confidentiality and Anonymous Reporting

Individuals may raise concerns confidentially or anonymously.

A confidential report is one where the individual provides their identity but asks the Company to keep it confidential. An anonymous report is one where the individual does not disclose their identity.

The Company will take reasonable steps to protect the identity of anyone raising a concern and will only share information with those who need it to assess, investigate or respond to the matter.

However, confidentiality cannot be guaranteed in all circumstances. Information may need to be disclosed where required by law, regulators, law enforcement agencies, the courts, or where necessary to properly investigate a concern. Where possible and lawful to do so, the Company will discuss this with the reporting individual beforehand.

Anonymous reports will be assessed and, where appropriate, investigated. However, anonymity may make it more difficult to gather further information, investigate the concern fully, or provide feedback.

The Company will not seek to identify an anonymous reporter unless there is a lawful and legitimate reason for doing so.

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

## 5.0 Protection from Detrimental Treatment

Bullying, harassment, victimisation, retaliation or any other form of detrimental treatment against an individual who raises a concern under this Policy is unacceptable.

The Company will not subject an individual to detriment because they have raised a concern in the public interest or participated in an investigation. Any person found to have retaliated against an individual for raising a concern may be subject to disciplinary action.

An individual who believes they have experienced detrimental treatment because they raised a concern should report this to the HR Team, a Director or the Chief Executive Officer.

A concern will not result in disciplinary action merely because it is not subsequently substantiated, provided the individual reported information they reasonably believed to be true at the time.

However, this protection does not extend to an individual who knowingly makes a false or malicious allegation. Such conduct may be addressed under the Company's disciplinary procedure. A concern will not be regarded as malicious solely because it is mistaken or cannot be substantiated.

## 6.0 Data Protection and Record Keeping

When a concern is raised under this Policy, the Company may process personal data relating to:

- The individual raising the concern.
- Individuals named or otherwise identified in the report.
- Witnesses and other persons connected with the matter.
- The assessment, investigation, findings and resulting actions.

Personal data will be processed in accordance with applicable data protection legislation and the Company's Data Protection Policy.

Information will be processed only where necessary for purposes including:

- Receiving and recording the concern.
- Assessing and investigating the information provided.
- Taking appropriate action.
- Protecting the rights and interests of affected individuals.
- Complying with legal, regulatory and contractual obligations.

Access to whistleblowing records, voicemail messages, transcriptions, emails and investigation material will be restricted to authorised individuals on a need-to-know basis.

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

Whistleblowing records will be stored securely and retained only for as long as necessary, taking account of the nature and outcome of the concern and any applicable legal, regulatory or contractual requirements. Records that are no longer required will be securely deleted or destroyed in accordance with the Company's retention arrangements.

Information relating to an allegation will be handled fairly. Where appropriate and lawful, individuals who are the subject of an allegation will be informed and given an opportunity to respond. Information that would identify the reporting individual will not be disclosed unless necessary and lawful.

## 7.0 External Disclosures

The Company encourages concerns to be raised through its internal reporting channels where this is appropriate. However, an individual may consider making a disclosure to an appropriate prescribed person or regulatory body where:

- They do not feel able to raise the concern internally.
- They reasonably believe that internal reporting is inappropriate.
- They believe that an internal concern has not been addressed appropriately.
- The relevant statutory requirements for an external disclosure are met.

Depending on the subject matter, prescribed persons and regulatory bodies may include:

- HM Revenue & Customs.
- The Financial Conduct Authority.
- The Competition and Markets Authority.
- The Health and Safety Executive.
- The Environment Agency.
- The Independent Office for Police Conduct.
- The Serious Fraud Office.
- The Information Commissioner's Office.

This list is not exhaustive. The appropriate prescribed person or body will depend on the subject matter of the concern.

Current guidance and the list of prescribed persons and bodies can be accessed through the [UK Government whistleblowing guidance](#).

Individuals may also wish to seek independent advice from a legal adviser, their trade union, Acas or the whistleblowing charity Protect before making an external disclosure.

Individuals should take care not to disclose confidential, classified, legally privileged or personal information unless permitted by law.

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

## 8.0 Responsibilities

### 8.1 Employees, Contract Workers and Other Reporting Individuals

Individuals raising concerns are expected to:

- Provide information honestly and based on information reasonably believed to be true.
- Provide as much factual detail as is reasonably available.
- Maintain appropriate confidentiality.
- Cooperate with an investigation where they have provided contact details and are asked to assist.
- Avoid conducting their own investigation or attempting to obtain information unlawfully.

### 8.2 HR Team

The HR Team is responsible for:

- Monitoring the dedicated whistleblowing email and voicemail inboxes.
- Ensuring appropriate cover arrangements are in place.
- Identifying reports marked as urgent and escalating them promptly.
- Maintaining appropriate confidentiality.
- Completing an initial assessment of each report.
- Escalating concerns to an appropriate Director, senior manager or other authorised person.
- Ensuring that actual or perceived conflict of interest involving those responsible for handling a report are documented and managed and that alternative arrangements made where necessary.
- Maintaining secure and accurate records.
- Retaining and disposing of records in accordance with the Company's data protection and retention arrangements.
- Supporting appropriate communication with an identified reporting individual where possible.

### 8.3 Directors and Senior Management

Directors and senior management are responsible for:

- Supporting an open culture in which concerns can be raised without fear of retaliation.
- Ensuring concerns escalated to them are assessed appropriately.
- Ensuring suitable investigations and remedial actions are authorised.
- Protecting reporting individuals from detrimental treatment.
- Ensuring significant matters are reported to relevant authorities where legally required or otherwise appropriate.

|                        |                       |                         |                    |                       |              |                      |            |
|------------------------|-----------------------|-------------------------|--------------------|-----------------------|--------------|----------------------|------------|
| <b>Document Number</b> | TSP-1022              | <b>Revisions Number</b> | 2026-v2.0          | <b>Classification</b> | Internal     | <b>Revision Date</b> | 09/10/2026 |
| <b>Document Name</b>   | Whistleblowing Policy | <b>Process Owner</b>    | Compliance Manager | <b>Retention</b>      | Indefinitely | <b>Release Date</b>  | 31/01/2023 |

## 8.4 Compliance Team

The Compliance Team is responsible for:

- Maintaining this Policy.
- Providing guidance on the operation of the whistleblowing arrangements.
- Supporting the review of the effectiveness of the reporting process.
- Coordinating necessary policy, website and internal communication updates.
- Supporting improvements identified through monitoring, investigations or lessons learned.
- Maintaining anonymised whistleblowing statistics and trend analysis for management review.

## 8.5 IT Team

The IT Team is responsible for:

- Maintaining the technical operation of the dedicated email and telephone reporting channels.
- Applying approved access permissions.
- Supporting the security, availability and appropriate retention of reporting information.
- Ensuring that changes to access permissions are authorised.
- Supporting testing of the reporting channels before implementation and following material changes.

IT personnel providing technical support must not access the content of whistleblowing reports unless specifically authorised and necessary for support, security or recovery purposes.

## 9.0 Policy Review

This Policy will be reviewed annually, or sooner where legal, regulatory, organisational, or operational changes require review.

Updates will be made as necessary to ensure the Policy remains effective, proportionate, and aligned with applicable legal and business requirements.