G2S GROUP

FEEL SAFE WITH US

WHISTLEBLOWING POLICY

POLICY STATEMENT

G2S-SOMS-POL-006

Version 2.0 | Effective 23 July 2026

Security Operations Management System (SOMS) / Integrated Management System

Conforms to ISO 18788:2015, ANSI/ASIS PSC.1-2022 and ISO 9001:2015

G2S GROUP

FEEL SAFE WITH US

CONTENTS

DOCUMENT CONTROL

Document Title	Whistleblowing Policy
Document Number	G2S-SOMS-POL-006
Version	2.0
Status	Approved
Effective Date	23 July 2026
Next Scheduled Review	23 July 2027
Supersedes	Version 1.0 (10-03-2026)
Document Owner	Compliance Officer
Approving Authority	Chief Executive Officer and Security Manager, G2S Group
Classification	Public
Applicable Management Systems	ISO 18788:2015 (SOMS) · ANSI/ASIS PSC.1-2022 · ISO 9001:2015 (QMS)

AMENDMENT HISTORY

Version	Date	Summary of Change	Author	Approved By
1.0	10-03-2026	Initial issue.	Compliance Officer	CEO / Security Manager
2.0	23-07-2026	Full revision for conformance with ISO 18788:2015, ANSI/ASIS PSC.1-2022 and ISO 9001:2015: published specific hotline number and email address for reporting, added RACI table, measurable KPIs, and document-control framework.	Compliance Officer	CEO / Security Manager

DISTRIBUTION

Distribution	Method
All employees, contractors, subcontractors and agency personnel	Induction pack; intranet; site notice boards; annual refresher training
Clients and prospective clients	Available on request; published on the G2S public website where indicated
Board of Directors and Senior Management	Management review pack; governance portal
Regulators and auditors	Provided on request for compliance verification

1. PURPOSE AND RATIONALE

The objective of this Policy is to encourage employees and third parties (contractors, partners, etc.) to report any concerns related to unethical, illegal, unsafe, or improper conduct within G2S. It applies to all employees, management, consultants, contractors, and stakeholders involved with G2S operations, outlining ways in which concerns about malpractice or wrongdoing can be raised at an early stage and in an appropriate way, in line with public-interest disclosure principles.

This Policy primarily addresses concerns where, due to malpractice, fraud, abuse, or other inappropriate acts or omissions, the interests of others or of G2S itself are at risk. Staff have a right, and a duty, to raise any matters of concern about security-service issues associated with the Company. The Policy provides a clear commitment that concerns will be taken seriously, and encourages staff to communicate concerns through the appropriate channels.

2. SCOPE

Whistleblowing includes the disclosure of information regarding malpractice, breaches of the Code of Ethics, criminal activity, corruption, abuse of authority, health and safety risks, environmental damage, or concealment of any of the above.

This Policy does not replace G2S's Complaints Procedure, which is used by customers to raise concerns about specific incidents, and does not apply to complaints about employment or how employees are treated (the Grievance Procedure or Harassment and Bullying Procedure should be used for such matters). Related G2S processes include the Incident Reporting Policy and

Procedure (incident reports may be submitted anonymously), the Serious Incident Policy and Procedure, and the Risk Management process.

This Policy is intended to cover serious public-interest concerns that fall outside the scope of other procedures. These are matters that, in the reasonable belief of the employee, are either happening now, have happened, or are likely to happen, including: a criminal offence; the breach of a legal obligation; a miscarriage of justice; a danger to the health and safety of an individual; damage to the environment; or the deliberate concealment of, or failure to report, any of the above.

3. WHISTLEBLOWING PROCESS

3.1 STEP 1: IDENTIFYING A REPORTABLE CONCERN

A whistleblower must have genuine and reasonable grounds to believe that a serious wrongdoing has occurred, is currently happening, or is likely to occur in the course of G2S's operations. Reportable concerns may relate to fraud, theft, embezzlement, corruption, bribery, misappropriation of assets, unauthorized use of company resources, breaches of occupational health and safety standards, violations of human rights, unethical conduct, discriminatory practices, sexual harassment, or any form of abuse or misconduct.

3.2 STEP 2: MAKING A DISCLOSURE

A concern may be submitted through the confidential and secure channels listed in Section 4, including the dedicated whistleblowing email, the anonymous drop boxes installed at company sites and high-risk field locations, or in person to the Compliance Officer, an authorized member of the Whistleblowing Committee, or trusted senior management. Disclosures should include a clear description of the issue, date and location, individuals involved or witnesses, and any supporting evidence.

3.3 STEP 3: ACKNOWLEDGEMENT OF REPORT

The Whistleblowing Officer acknowledges receipt of the report within 5 working days, unless the report was made anonymously or acknowledgment would risk exposing the whistleblower or jeopardizing an investigation, in which case the case proceeds directly to review. The whistleblower's identity is protected throughout the process unless express consent is given to disclose it, or disclosure is legally mandated.

3.4 STEP 4: PRELIMINARY REVIEW

The Whistleblowing Officer conducts a preliminary review within 10 working days of receipt to determine whether the matter falls within scope and whether the allegation is sufficiently credible to warrant a formal investigation. Matters relating to routine grievances or matters better handled by Human Resources or Security are referred accordingly.

3.5 STEP 5: FORMAL INVESTIGATION

Where warranted, the Compliance Department or an appointed Whistleblowing Investigation Committee initiates a formal investigation, led by personnel independent of the concern raised, tasked with ensuring impartiality and due diligence. The investigation is completed within 30 calendar days, although extensions may be granted in complex cases provided reasons for delay are documented. Confidentiality of all individuals is maintained throughout.

3.6 STEP 6: OUTCOME AND RECOMMENDATIONS

A formal report is prepared summarizing the facts, findings, and recommendations, reviewed by Senior Management and, where applicable, Legal Counsel. Substantiated allegations may result in disciplinary action ranging from formal warnings to contract termination or legal referral. Where no wrongdoing is confirmed, the case is closed and records retained for accountability.

3.7 STEP 7: FEEDBACK TO THE WHISTLEBLOWER

Where feasible and appropriate, the whistleblower is provided with feedback on the status and outcome of the investigation, in a manner that protects the confidentiality and rights of other parties. Feedback to anonymous whistleblowers is provided only where a secure method of communication was used.

3.8 STEP 8: RECORDKEEPING AND MONITORING

All whistleblowing reports, investigation notes, outcomes, and corrective actions are securely logged in a centralized whistleblowing register managed by the Compliance Department, including date of receipt, nature of concern, persons involved, summary of findings, and resolution status. Records are retained for a minimum of five years and are accessible only to authorized personnel.

4. REPORTING CHANNELS

G2S provides the following confidential and accessible channels for raising concerns:

- Confidential whistleblowing hotline: +252-634-000290
- Dedicated whistleblowing email: grievances@g2sgroups.com
- Anonymous whistleblower forms (physical or digital) available at all sites
- Physical complaint / drop boxes installed at company offices and high-risk field locations
- In-person reporting to the Compliance Officer or an authorized member of the Whistleblowing Committee
- Direct reporting to Human Resources

Reports can be made verbally, in writing, or anonymously, and G2S encourages the use of whichever channel the whistleblower feels most comfortable with.

5. CONFIDENTIALITY AND ANONYMITY

Confidentiality is a cornerstone of this Policy. All reports are handled with the highest degree of discretion, and efforts are made to safeguard the identity of the whistleblower at every stage. Individuals are permitted to make anonymous reports, and systems are in place to protect anonymity unless disclosure is required by law or necessary to conduct a fair and thorough investigation, in which case the whistleblower is informed of any disclosures necessary to move forward.

6. PROTECTION AGAINST RETALIATION

G2S enforces a strict zero-tolerance policy against retaliation. Any form of reprisal, direct or indirect, against a whistleblower who raises concerns in good faith is a serious violation of company policy and will result in disciplinary action, including termination, demotion, intimidation, harassment, discrimination, or any adverse employment consequence. Whistleblowers are assured they will not suffer negative consequences for coming forward with a genuine concern.

7. INVESTIGATION PROCESS

G2S initiates a structured, confidential, and impartial investigation process upon receiving a report, beginning with initial screening by the Compliance Officer or Whistleblowing Focal Point to verify scope, assess credibility, and determine severity and legal implications. Depending on complexity, cases may be assigned

to an internal investigation team, an external third-party investigator, or a specially appointed Whistleblowing Committee. In highly sensitive cases (fraud, physical abuse, inappropriate use of force, violations of humanitarian law), G2S may engage independent experts or legal counsel. G2S maintains a firm non-retaliation policy throughout; any individual under investigation is treated fairly and given the opportunity to respond to allegations.

8. FALSE ALLEGATIONS

While G2S encourages the reporting of suspected wrongdoing, malicious or knowingly false allegations made with intent to harm another person, disrupt operations, or manipulate outcomes may be subject to disciplinary measures, including termination or legal recourse. This is distinct from, and does not discourage, good-faith reporting that later proves unfounded.

9. ROLES AND RESPONSIBILITIES

Role	Responsibility under this Policy
Compliance Officer / Whistleblowing Officer	Central coordinator of the whistleblowing framework: receives reports, conducts or initiates preliminary assessments, escalates matters for investigation, maintains accurate records, ensures timelines are met, and monitors protection of the whistleblower from retaliation.
Human Resources Department	Provides protective and remedial support to whistleblowers, particularly for workplace-related concerns; ensures no victimization or adverse changes in terms of employment.
Senior Management	Holds ultimate accountability for reinforcing the values underpinning this Policy; reviews investigation outcomes and implements corrective action; allocates resources to Compliance and HR.
Whistleblowing Committee / Internal Investigations Unit	Manages the full investigation cycle for sensitive, complex, or high-stakes allegations, operating independently and objectively.
All personnel	Report suspected wrongdoing in good faith; maintain confidentiality of information obtained during any process in which they participate.

10. AWARENESS AND TRAINING

All employees, including security personnel, administrative staff, and support teams, are introduced to this Policy during onboarding. G2S delivers periodic refresher training covering policy updates, evolving risks, and case-based scenarios, with tailored briefings for frontline personnel deployed to high-risk or remote locations. Managers and supervisors receive additional training on responding appropriately when a concern is raised, including how to protect whistleblowers and escalate concerns confidentially.

11. MEASURABLE OBJECTIVES AND MONITORING

Objective	Measurable Target / KPI	Review Frequency
Acknowledgment of reports	100% within 5 working days (except where omission is required to protect anonymity)	Monthly
Preliminary review completed	100% within 10 working days	Monthly
Formal investigations completed	100% within 30 calendar days (documented extensions permitted)	Quarterly
Substantiated retaliation cases	0 (zero target)	Quarterly
Training completion (induction and refresher)	≥ 95% of personnel	Annually

The whistleblowing register is reviewed periodically by the Compliance Department to monitor patterns, evaluate systemic risks, and support broader compliance oversight, and is a standing input to the annual SOMS management review.

12. MONITORING AND COMPLIANCE

The Compliance Department holds primary responsibility for overseeing execution of this Policy, maintaining a secure, up-to-date register of all reported concerns, and tracking the status and outcomes of investigations. G2S conducts an annual audit of the whistleblowing system, assessing whether reporting channels remain accessible and confidential, whether staff are adequately trained, and whether organizational response reflects fairness and due process. Findings are reviewed by the Executive Committee and necessary adjustments implemented as part of continuous improvement.

13. RELATED DOCUMENTS

- G2S-SOMS-POL003- Code of Ethics / Code of Conduct
- G2S-SOMS-POL004- Anti-Fraud, Bribery and Corruption Policy
- G2S-SOMS-POL005- Conflict of Interest Policy
- G2S Incident Reporting Policy and Procedure
- G2S Grievance Procedure and Harassment and Bullying Procedure

APPROVAL AND ENDORSEMENT

This document has been reviewed and approved by G2S Group leadership and is effective from the date shown below. It forms part of the G2S Security Operations Management System (SOMS) / Integrated Management System and is maintained in conformance with ISO 18788:2015, ANSI/ASIS PSC.1-2022, and ISO 9001:2015.

Approved By	Date
Abdishakur Hassan Kayd Security Manager, G2S Group	23-07-2026

Approved By	Date
Kader Abdi Daher Chief Executive Officer, G2S Group	23-07-2026

G2S GROUP

FEEL SAFE WITH US

Contact Us :

+252 63 4000290

info@g2sgroups.com

www.g2sgroups.com

Muj Abdilahi Askar Rd. Southwest of
Maansoor Hotel, Hargeisa, Somaliland