GLOBAL STAR
SECURITY SERVICES
YOUR SHIELD OF SECURITY

SECURITY POLICY		
POLICIES & PROCEDURES		
Author: Operations Dept	**Policy Code**: GSS/HR 013/25	**Source:**
Version: Version 1	**Effective Date:** November 2025	**Revision Date:** November 2026
Policy Type: Workplace Policy	**Policy Owner:** Global Star Security Services	**Ref No:**
Prepared By: Operations Dept	**Reviewed By:** Managing Director	**Authorized By:** Chief Executive Officer

TABLE OF CONTENTS

1. PREAMBLE

Global Star Security Services (GSS) is committed to delivering reliable, ethical, and high-quality security solutions that protect people, assets, and operations across all environments. As a responsible security provider, GSS upholds the principles of professionalism, legality, respect for human rights, and operational excellence. This Security Policy establishes the standards, responsibilities, and procedures necessary to ensure the safe, effective, and compliant execution of all security activities conducted by GSS personnel.

---

2. PURPOSE

The purpose of this policy is to:

- Establish uniform security standards across all GSS operations.
- Ensure the safety of employees, clients, visitors, and stakeholders.
- Protect property, assets, sensitive information, and operational infrastructure.
- Define clear responsibilities for personnel at all levels.
- Promote compliance with national laws, industry standards, and client requirements.
- Support a secure, resilient, and well-managed operational environment.

---

3. SCOPE

This policy applies to:

- All GSS employees, both operational and administrative
- Contractors, subcontractors, and consultants
- Temporary staff, interns, and volunteers
- All GSS facilities, vehicles, equipment, and operational sites
- All client sites where GSS provides services

It includes physical security, personnel security, information security, operational security, and emergency management.

4. KEY PRINCIPLES

GSS adheres to the following foundational principles:

Legality

All operations comply with local, national, and international laws, including licensing and regulatory requirements.

Ethical Conduct

Personnel must act with integrity, respect, and professionalism at all times.

Human Rights Protection

GSS upholds international human rights standards and ensures the dignity and safety of all individuals.

Confidentiality

Sensitive information is protected against unauthorized access or disclosure.

Risk Management

Decisions are guided by continuous threat and risk assessment.

Zero Tolerance for Misconduct

GSS maintains zero tolerance for corruption, abuse of force, sexual exploitation, theft, and other unethical behavior.

---

5. RESPONSIBILITIES

Management

- Provide strategic direction and oversight.
- Ensure adequate resources, training, and supervision.

- Approve security plans and risk management strategies.
- Promote a strong security culture.

Supervisors and Team Leaders

- Enforce policies and operational procedures.
- Conduct briefings, debriefings, and inspections.
- Identify security risks and report concerns.
- Support and mentor security personnel.

Security Personnel

- Follow all standard operating procedures (SOPs).
- Remain alert, disciplined, and professional.
- Report incidents immediately.
- Protect client assets and uphold company values.

All Employees

- Comply with policy requirements.
- Safeguard company property and information.
- Follow emergency and evacuation procedures.
- Report suspicious activity or breaches.

---

6. SECURITY STANDARDS

Physical Security

- Access control systems must be implemented and monitored.
- Visitors must be registered, screened, and escorted where necessary.
- Perimeters, gates, and barriers must be secured and regularly inspected.
- Security lighting and CCTV systems must be operational and maintained.

Personnel Security

- Background checks must be performed during recruitment.
- Staff must carry valid IDs while on duty.

- Unauthorized personnel are not permitted in restricted areas.
- Staff must follow uniform and equipment regulations.

Information Security

- Confidential documents must be stored securely.
- Electronic systems must be password-protected.
- Unauthorized sharing of client or company information is prohibited.
- Personnel should follow secure communication protocols.

Operational Security (OPSEC)

- Operational plans must be protected from unauthorized access.
- Movement of teams, assets, and vehicles must be controlled and documented.
- Sensitive information must be shared only on a need-to-know basis.
- Operational risks must be evaluated daily.

Use of Force

- Personnel may only use force that is lawful, reasonable, and proportionate.
- Firearms and equipment must be used only by trained and authorized staff.
- All use-of-force incidents must be reported immediately.

---

7. INCIDENT REPORTING & RESPONSE

- All incidents, threats, or breaches must be reported to supervisors immediately.
- An Incident Report Form must be completed for every security incident.
- Serious incidents must be escalated to management without delay.
- Investigations must be conducted promptly and fairly.
- Corrective actions must be implemented to prevent recurrence.

---

8. TRAINING & COMPETENCY

GSS will ensure that all security personnel receive:

- Induction and refresher training
- Training on use of force, de-escalation, and human rights
- Emergency and first-aid training
- Radio communication and incident reporting skills
- Site-specific training based on risk assessments

Training records must be maintained and reviewed regularly.

---

9. EMERGENCY MANAGEMENT

GSS will maintain up-to-date emergency procedures including:

- Fire safety
- Evacuation plans
- Medical emergencies
- Natural disasters
- Security breaches or attacks

All employees must be familiar with site-specific emergency protocols.

---

10. COMPLIANCE AND AUDITING

- Regular audits will assess compliance with this policy.
- Non-compliance will result in corrective actions or disciplinary measures.
- Findings and lessons learned will inform continual improvement.

---

11. CONFIDENTIALITY AND DATA PROTECTION

All information gathered during security operations must be handled responsibly and according to GSS confidentiality requirements. Unauthorized disclosure is strictly prohibited.

---

12. REVIEW OF THE POLICY

This policy will be reviewed annually or sooner if:

- Operational requirements evolve
- Legal or client requirements change
- New risks or technologies emerge
- Internal audits recommend adjustments