Security Policy

For Stanford & Green Limited

1. Purpose

The purpose of this Security Policy is to safeguard:

- Employees, enforcement agents, and contractors.
- Assets, equipment, vehicles, and seized goods.
- Personal and sensitive information relating to debtors, clients, and court orders.

Stanford & Green Limited is committed to maintaining high standards of security to protect people, information, and operations.

2. Scope

This Policy applies to:

- All employees, agents, directors, and contractors.
- All office sites, storage facilities, vehicles, and any operational locations.
- All physical and digital assets owned or managed by Stanford & Green Limited.

3. Physical Security

3.1. Offices and Storage Facilities

- Offices must be secured with controlled access (e.g., keycards, locks).
- Seized goods must be stored in secure facilities with limited authorised access.
- CCTV surveillance must be operational where legally permitted.
- Alarm systems must be installed and maintained.

3.2. Vehicles and On-Site Security

- Vehicles must be locked when unattended and equipped with tracking systems.
- Seized goods must not be left unattended without secure storage.
- Enforcement agents must assess personal safety risks before visits and may work in pairs if required.
- Body-worn video (BWV) cameras should be used when appropriate and legally compliant.

4. Information and Data Security

4.1. Data Handling

- Debtor and client information must be treated as confidential.
- Hard copies of sensitive documents must be locked away when not in use.
- Digital records must be stored securely on encrypted systems.

4.2. Access Control

- Access to databases and case files must be restricted to authorized personnel only.
- Unique usernames and passwords must be used for all IT systems.
- Access rights must be reviewed regularly.

4.3. Communication

- Mobile devices and laptops must be password-protected.
- Emails containing sensitive data must be encrypted.
- Personal data must not be shared via unsecured channels (e.g., unencrypted email, public Wi-Fi).

5. Incident Management

- All security breaches (physical or digital) must be reported immediately to management.
- An investigation will be launched for any reported breach.
- Major incidents must be escalated to the company’s Data Protection Officer (DPO) and/or Security Manager.

6. Employee Responsibilities

- Always follow all security procedures.
- Challenge or report unauthorised persons on company premises.
- Protect personal security while conducting enforcement actions.
- Maintain confidentiality when dealing with sensitive debtor information.
- Report any suspicious activity, loss, or theft immediately.

7. Training

- Security training (including personal safety, cyber-security basics, and information handling) is mandatory.
- All new staff/personnel must complete security induction training within 30 days.
- Ongoing refresher training must be conducted annually.

8. Policy Review

This Security Policy will be reviewed annually or sooner if:

- There is a significant security incident.
- New security threats emerge.
- Legal or regulatory changes require updates.

Signed: Martin Stanford – Managing Director

8 January 2026

Summary for Enforcement Agents

✅ Keep yourself, your vehicle, and seized goods secure at all times.
✅ Protect debtor and client information — no unsecured documents or conversations.
✅ Immediately report any theft, attack, data breach, or suspicious behaviour.
✅ Use encryption and strong passwords for all devices and communications.