**Security Plan Template (Operating Centre, Vehicles, and People)**

**[COMPANY NAME]** **Security Plan**

**1.0 Purpose** This Security Plan details the measures implemented by [Company Name] to protect our people, vehicles, premises, and customers' goods from theft, vandalism, and other malicious acts. This plan is essential for maintaining operational integrity, ensuring staff safety, and meeting the requirements of our Operator's Licence.

**2.0 Scope** This plan applies to all company premises, vehicles (owned and subcontracted while on company business), employees, agency staff, and visitors.

**Part A: Operating Centre Security**

**2.1 Site Perimeter & Access Control**

* **Fencing:** The operating centre at [Your Address] is secured by [Describe fencing, e.g., 2.4m high palisade fencing, chain-link fence]. Fencing is inspected [e.g., weekly] for damage.
* **Gates:** The main access gate is [Describe gate, e.g., a lockable steel sliding gate]. It is kept locked outside of operating hours of [State hours, e.g., 07:00 - 18:00, Monday-Friday]. Responsibility for locking and unlocking lies with [State role, e.g., the first person in and the last person to leave].
* **Access for Visitors/Drivers:** All visitors and non-company drivers must report to reception [or designated point], sign in the visitor log, and be issued with a visitor's pass. They must be escorted in secure areas.

**2.2 Lighting & CCTV**

* **Lighting:** The site is equipped with [Describe lighting, e.g., high-level floodlights covering the yard and parking areas]. The lighting is sensor-activated/timer-controlled and checked [e.g., weekly] to ensure functionality.
* **CCTV:** A CCTV system is in operation with cameras covering [Describe camera locations, e.g., the gate, fuel island, vehicle parking area, and loading bay]. Recordings are kept for [e.g., 30] days. The system is monitored by [e.g., the Transport Manager] and maintained by [Name of service provider]. Signs are in place to notify people that CCTV is in operation.

**2.3 Key Security**

* All keys for buildings and vehicle compounds are managed through a secure key cabinet located in [Location, e.g., the Transport Office].
* Access to the key cabinet is restricted to authorised personnel: [List roles, e.g., Directors, Transport Manager].
* A log must be signed to issue and return keys.

**Part B: Vehicle & Load Security**

**3.1 Vehicle Security Devices**

* All vehicles are fitted with: [List devices, e.g., engine immobilisers, tracking/telematics systems, steering wheel locks, anti-siphon fuel devices].
* Trailers are secured with [e.g., kingpin locks, high-security container seals] when parked or loaded.

**3.2 Parking Procedures**

* **On-Site:** When parked on-site overnight, vehicles should be parked [Describe strategy, e.g., defensively, with larger vehicles blocking smaller ones, or with loading doors backed up against a wall]. All vehicles must be locked, and windows closed.
* **Off-Site / Overnight:** Drivers must only use approved, secure parking locations for overnight stops. A list of approved sites is [State where, e.g., available from the Transport Office, uploaded to the driver's tablet]. Drivers must inform the Transport Office of their overnight location. Drivers must never discuss their load or route in public.

**3.3 Load Security**

* Drivers must not leave a loaded vehicle unattended unless in a designated secure parking area.
* High-value loads require [Describe extra measures, e.g., routing away from known hotspots, use of a second crew member, enhanced tracking, numbered seals to be checked at each stop].
* Documentation (CMRs, delivery notes) should not be left visible in the cab.

**3.4 Vehicle Key Security**

* Vehicle keys must never be left in the ignition of an unattended vehicle.
* At the end of a shift, drivers must hand their keys directly to the Transport Manager or place them in the secure key cabinet. Keys must not be taken home without prior authorisation.

**Part C: Personnel Security**

**4.1 Staff Vetting & Training**

* All prospective drivers and staff with access to secure areas are subject to pre-employment checks, including [e.g., reference checks for the last 5 years, driving licence check, right-to-work check].
* All staff receive security awareness training as part of their induction, covering topics such as "see something, say something," recognising suspicious behaviour, and reporting procedures. This is refreshed [e.g., annually].

**4.2 Roles & Responsibilities**

* All staff are responsible for being vigilant and reporting any security concerns or breaches immediately to the Transport Manager.
* The **Transport Manager [or other designated role]** is the designated Security Officer, responsible for maintaining and reviewing this plan.

**4.3 Incident Reporting Procedure**

* In the event of a security incident (e.g., theft of vehicle, break-in):
  1. Ensure personal safety first.
  2. Contact the emergency services (Police on 999) if a crime is in progress or has just occurred.
  3. Report the incident immediately to the Transport Manager on [Phone Number].
  4. Preserve any evidence if it is safe to do so.
  5. Complete a company incident report form as soon as possible.
* The Transport Manager will escalate the report to the Directors and, if required, the DVSA and the company’s insurers.

**5.0 Policy Review** This Security Plan will be reviewed annually, or in response to any security incident, to ensure it remains effective.

**Signed:** ................................................................. **Name:** [Name of responsible person, e.g., Transport Manager/Director] **Position:** [Position] **Date:** [Date] **Next Review Date:** [Date]