

Human Resources Policies & Procedures

Subject: Security Policy
Date: 06 November 2025

Page: 1/4

Title: Security Policy	Written By: S Curtis
SOP No: Uni-SMS012	Approved By: C Chadwick
Version Number: 3.0	Date of Issue: 06/11/2025
Supersedes: 2.0	

Security Policy

Introduction

Uniserve’s business is primarily concerned with transporting customers’ freight. Much of the freight is moved on our own and others’ transport and through our own and others’ warehousing facilities and must be received, handled and delivered to them safely, securely and in good condition.

This security policy is :

- consistent with other organizational policies;
- consistent with the organization’s overall security risk assessment;
- provides for its review in case of the acquisition of, or a merger with, other organizations, or other changes to the business scope of the organization which could affect the continuity or relevance of the security management system;
- describes and allocate primary accountability and responsibility for outcomes;
- available as documented information;
- communicated within the organization;

Warehouse and storage

Keeping the freight, premises & group assets secure is paramount.

As a result, all Uniserve staff should follow these simple rules. **Managers and supervisors are responsible for ensuring that staff are adequately trained, are aware of and comply with these rules. All documented instructions within the groups Security management system (SMS) must be adhered to.**

Any suggestions about improvements to our security procedures or measures should be made to the appropriate director.

General Rules

- Where required for external certification requirements. All staff will have references checked by HR and will be employed subject to satisfactory references and Criminal Disclosure and Baring Service (DBSs).
- Staff refusing to give appropriate references or to comply with consent to DBS checks will be dismissed.
- Staff receiving unsatisfactory references or DBS checks will be dismissed.
- All buildings must be kept secure at all times, especially at the end of the working day.

Effective date	Reference	Page		Document Classification
06/11/2025	SMS012	1 of 4	V3.0	Internal Use

Human Resources Policies & Procedures

Subject: Security Policy
Date: 06 November 2025

Page: 2/4

- Gates, doors & shutters must be kept closed and locked during the day when not in use. Doors must not be kept 'on the latch'.
- Premises should only be accessed from the main reception area or from the Drivers reception areas located to the rear of the facility, where appropriate.
- ID cards will be issued to staff with specific access rights assigned dependant on job description and working area.
- Staff are required to present their ID cards at the on-line reader at the start and end of their working day (at applicable sites).
- Staff must always present their cards at on-line readers and door card readers when entering or leaving an area controlled by access control card technology. They must never 'tail gate' other staff or leave doors propped open.
- Lending or borrowing ID cards is a disciplinary offence and could result in dismissal.
- Uniserve staff should wear their photo ID security badges at all times.
- Lost or damaged cards must be reported to HR within 24 hours. Replacement cards will be issued at a cost to the staff member (which will be deducted from their salary)
- Staff who forget their ID card will be asked to return home to retrieve it and will have the time taken added to the end of their working day or pay deducted accordingly
- All visitors (other than regular delivery personnel) must be signed in and signed out
- Visitors must always be accompanied by a member of Uniserve staff
- Strangers on site who are unaccompanied by Uniserve staff and/or who are not, must be challenged, asked for identification and escorted politely to a supervisor or manager for verification
- Anyone acting suspiciously on site (including staff) must be reported immediately to a supervisor or manager. Who in turn will notify the on-site security Manager or Supervisor (FMDC & Tilbury). All security incidents must be lodged either directly or via the on-site security team into the groups Evoxix Assure reporting platform.
- Staff who are unsure about any security measures, or who are aware of potential or actual security breaches, must report them to a supervisor or manager. If the breach has been committed by their supervisor or manager (or a director), then they should contact the Director of Human Resources (or the Managing Director, if the breach has been committed by the Director of HR), who will treat their communication in confidence and will conduct an appropriate investigation. Anonymous communications will not be actioned

When finishing work, shutting and locking **any** premises after work;

- All confidential documents and documents where unauthorised access could result in a security breach or loss of commercially sensitive information, must be locked away
- Laptops must be locked away
- All internal lights must be turned off
- All keys must be locked away securely
- Any internal fire doors must be shut
- **All** doors must be shut and locked
- Alarms must be set by key-holders after the building has been made secure

Effective date	Reference	Page		Document Classification
06/11/2025	SMS012	2 of 4	V3.0	Internal Use

Human Resources Policies & Procedures

Subject: Security Policy
 Date: 06 November 2025

Page: 3/4

Warehouse Specific Rules

In addition to the above 'General Rules', the following apply;

- All freight must be appropriately safeguarded against unauthorised access or pilfering.
- All visitors and staff must wear a high visibility jacket when in the warehouse.
- All internal processes and procedures for stock control both inbound and outbound must be fully followed as per the appropriate working procedure.
- When shutting a warehouse after work;
 - All freight handling equipment and valuable materials must be stored inside the warehouse and the keys locked away securely.
 - All shutters must be locked and secured
 - Any freight vehicles parked on Uniserve premises must be left with sheets tied back and keys removed.

For staff processing or handling Airfreight freight

Airfreight security, because of the threat to Aviation Security, is governed by its own set of additional detailed regulations. Uniserve's Airfreight Security Manager, in conjunction with HR, will ensure that all staff who deal in any way with Airfreight are appropriately trained in the Aviation Security Procedures, in addition to this Security policy.

All staff issued with permanent/ temporary and/or airport ID passes will be subject to a DBS as part of the airport operator's security regime.

Security Audits

The Security manager will audit procedures and practices at least annually and will report any breaches to the relevant Site General Manager.

The Group reserves the right to conduct personal searches (which includes bags and vehicles) on a random basis as part of our commitment to the security of the goods on our premises.

Any breaches of these rules will result in disciplinary action and could result in dismissal.

Transport of loads – Customer and group assets.

All drivers must follow all regulations as appropriate to SWP 039 & SWP 035 Vehicle and Load Security. In addition to Toolbox Talk "The importance of HGV Drivers Parking in a Secure location. Failure to comply with these rules will result in disciplinary action.

All vehicles entering or exiting the following sites (Tilbury & FMDC) must have completed that sites specific vehicle process as listed below.

Tilbury: Addition of details to the Live vehicle sheet both upon entrance and exit prior to arrival or departure.

FMDC: Upon arrival a Unique FMDC reference number must be supplied to gain entrance. Upon

Effective date	Reference	Page		Document Classification
06/11/2025	SMS012	3 of 4	V3.0	Internal Use

Human Resources Policies & Procedures

Subject: Security Policy
Date: 06 November 2025

Page: 4/4

departure details of the departure must be noted by the security point to confirm departure from the site.

Company acquisition or merger.

This security policy will be provided for its review in case of the acquisition of, or a merger with, other organizations, or other changes to the business scope of the organization which could affect the continuity or relevance of the security management system;

Document review and update.

This document shall be reviewed at least yearly. Or upon process change and accreditation requirement. Version control will be applied. Upon update the new version will be added to the Uniserve Website by the marketing department. On site copies held upon on-site SHEQ notice boards will be swapped by the sites security team. A group wide email will also be sent by HR to all employees confirming there have seen a change to the security policy. And it is available to view by all employees either on the Uniserve Website or site SHEQ notice boards.

Signed By:



Print: Mr Chris Chadwick
Dated: 06/11/2025

Effective date	Reference	Page		Document Classification
06/11/2025	SMS012	4 of 4	V3.0	Internal Use