



DANGEROUS GOODS SECURITY PLAN

CONTENTS

	Page Number
Front cover	1
Contents	2
Company Security Policy Statement	3
Section 1. Business details	4
	5
	6
	7
	8
	9
Section 2. Management of Security	9
	10
	11
	12
Section 3. Communication	12
	13
	14
Section 4. Measures of Site Security	14
	15
Miscellaneous information	15
Annex A - List of people responsible for the management of security issues and their duties	15
Annex B - List of people authorised to handle high consequence dangerous goods	15
Annex C - Security risk assessment matrix UK offices	16
Annex D - Risk assessment of the security of HCDG during Handling, Storage & Transport	17
Annex E - Details of people who have access to the security plan	18
Annex F - Record of reviewing and updating security plan	19
	20
Annex G - Site Plans	20
Annex H - Desktop exercises	21
	22

COMPANY SECURITY POLICY STATEMENT

It is M&S Logistics policy to aim to achieve the highest standard in respect of security in the carriage of dangerous goods. The requirement as a tank container operator engaged in the carriage of high consequence dangerous goods to adopt, implement and comply with a security plan has been incorporated in our Business Management System.

The security plan contains all the required elements including but not limited to the following:

- Specific allocation of security responsibilities to competent and qualified persons
- Records of dangerous goods involved
- Review of current operations and assessment of security risks
- Clear statement of measures to be taken to reduce security risks including training and new employee verification etc.
- Effective and up to date procedures for reporting and dealing with security threats and incidents
- Company cyber-security measures which are closely monitored and regularly updated with state-of-the-art firewall protecting all offices
- Procedures for the evaluation, testing, periodic review and update of the security plan
- Measures to ensure the physical security of transport information
- Distribution of information relating to transport operation contained in the security plan is limited to those who need to have it.

2026 Security Objectives

- To achieve zero security incidents worldwide.

Company security objectives are reviewed at the 6 monthly Business Management System Review Meeting and adjustments made if appropriate.

Telephone and e-mail contact details for site security applies to

UK	Sandbach	Tel: +44 (0) 1270 757928 E-mail ianf@mslogisticsltd.com
	Billingham	Tel: +44 (0) 1642 343435 E-mail martinc@mslogisticsltd.com
Europe	Rotterdam	Tel: +31 (0) 1866 30222 E-mail jacog@mslogisticsltd.com
	Houston	Tel: 001 281 915 0241 E-mail wimr@mslogisticsltd.com
Americas	Durban	Tel: +27 (0) 31 312 3212 E-mail kreasonp@mslogisticsltd.com
	Singapore	Tel : +27 (0) 31 312 3212 E-mail kreasonp@mslogisticsltd.com

- 5. Name of nominated security co-ordinator** Mr Ian Ferguson
- 6. Contact details for this security co-ordinator** Tel: +44 (0) 1270 757928
E-mail ianf@mslogisticsltd.com
- 7. Training given to security co-ordinator**
He has received Security training based on the Guidance issued by the DfT on Dangerous Goods Security Training.
- 8. Name of the Dangerous Goods Security Advisor (DGSA)** Mr John Frederick Harris
Certificate No. 2814071/240418

- 10. Overview of current operations**
An office based international tank container operator providing transportation of hazardous and non-hazardous bulk liquids using approved service providers. Head office is situated in Sandbach, UK with regional offices in Rotterdam, Houston, Durban, and Singapore. The purpose and scope of this security plan is to ensure that the security requirements of ADR and the IMDG Code for HCDG are fully implemented for all such movements we carry out.

11. List of dangerous goods

Classes 3, 4.1, 5.1, 6.1, 8 and 9 are transported of which the following list of HCDGs have been accepted for transport in recent years:

M&S Logistics - High Consequence Dangerous Goods (HCDG)			
Proper Shipping Name	UN Number	Class	Packing Group
ACETALDEHYDE	1089	3	I
ACRYLONITRILE, STABILIZED	1093	3	I
ALLYL ALCOHOL	1098	3	I
ALLYL CHLORIDE	1100	3	I
1-PENTENE	1108	3	I
CARBON DISULPHIDE	1131	3	I
DIETHYL ETHER (ETHYL ETHER)	1155	3	I
ISOPRENE, STABILIZED	1218	3	I
ISOPROPYLAMINE	1221	3	I
METHYL FORMATE	1243	3	I
PENTANES Liquid	1265	3	I
PROPYLENE OXIDE	1280	3	I
VINYL ETHYL ETHER, STABILIZED	1302	3	I
SODIUM	1428	4.3	I
ACETONE CYANOHRIN, STABILIZED	1541	6.1	I
CHLOROPICRIN	1580	6.1	I
DIMETHYL SULPHATE	1595	6.1	I
BROMINE	1744	8	I
FLAMMABLE LIQUID, N.O.S.	1993	3	1
MORPHOLINE	2054	8	I
METHYL CHLOROACETATE	2295	6.1	I
2-CHLOROPROPANE	2356	3	I
ETHYL MERCAPTAN	2363	3	I
FURAN	2389	3	I
AMINES, LIQUID, CORROSIVE, FLAMMABLE, N.O.S.	2734	8	I
POLYAMINES, LIQUID, CORROSIVE, N.O.S.	2735	8	I
TOXIC LIQUID, ORGANIC, N.O.S.	2810	6.1	I
TOXIC SOLID, ORGANIC, N.O.S.	2811	6.1	I
CORROSIVE LIQUID, FLAMMABLE, N.O.S.	2920	8	I
TOXIC LIQUID, CORROSIVE, ORGANIC, N.O.S.	2927	6.1	I
CORROSIVE LIQUID, BASIC, ORGANIC, N.O.S.	3267	6.1	1
HYDROCARBONS, LIQUID, N.O.S.	3295	3	I
TOXIC BY INHALATION LIQUID, N.O.S.	3382	6.1	I
MOTOR FUEL ANTI-KNOCK MIXTURE, FLAMMABLE	3483	6.1	I
ACETONE	1090	3	II
PENTANOLS	1105	3	II
AMYL CHLORIDES	1107	3	II
BENZENE	1114	3	II
BUTANOLS	1120	3	II
BUTYL ACETATES	1123	3	II
N-BUTYLAMINE	1125	3	II
1-BROMOBUTANE	1126	3	II

CHLOROBUTANES	1127	3	II
BUTYRALDEHYDE	1129	3	II
COAL TAR DISTILLATES, FLAMMABLE	1136	3	II
CYCLOHEXANE	1145	3	II
CYCLOPENTANE	1146	3	II
1,2-DICHLOROETHYLENE	1150	3	II
DIETHYLAMINE	1154	3	II
DIETHYL KETONE	1156	3	II
DIISOPROPYLAMINE	1158	3	II
DIISOPROPYL ETHER	1159	3	II
DIMETHYLAMINE, AQUEOUS SOLUTION	1160	3	II
DIMETHYL CARBONATE	1161	3	II
DIMETHYL SULPHIDE	1164	3	II
DIOXANE	1165	3	II
DIOXOLANE	1166	3	II
ETHANOL (ETHYL ALCOHOL) or ETHANOL SOLUTION (ETHYL ALCOHOL SOLUTION)	1170	3	II
ETHYL ACETATE	1173	3	II
ETHYLBENZENE	1175	3	II
ETHYL BUTYL ETHER	1179	3	II
ETHYLENE DICHLORIDE	1184	3	II
ETHYL METHYL KETONE (METHYL ETHYL KETONE)	1193	3	II
GASOLINE	1203	3	II
HEPTANES	1206	3	II
HEXANES	1208	3	II
ISOBUTYL ACETATE	1213	3	II
ISOPROPANOL (ISOPROPYL ALCOHOL)	1219	3	II
ISOPROPYL ACETATE	1220	3	II
KETONES, LIQUID, N.O.S.	1224	3	II
METHANOL	1230	3	II
METHYL ACETATE	1231	3	II
METHYLAL	1234	3	II
METHYLAMINE, AQUEOUS SOLUTION	1235	3	II
METHYL BUTYRATE	1237	3	II
METHYL ISOBUTYL KETONE	1245	3	II
METHYL METHACRYLATE MONOMER, STABILIZED	1247	3	II
OCTANES	1262	3	II
PAINT RELATED MATERIAL	1263	3	II
PENTANES, liquid	1265	3	II
PETROLEUM CRUDE OIL	1267	3	II
PETROLEUM DISTILLATES, N.O.S.	1268	3	II
n-PROPANOL (PROPYL ALCOHOL, NORMAL)	1274	3	II
PROPIONALDEHYDE	1275	3	II
n-PROPYL ACETATE	1276	3	II
PYRIDINE	1282	3	II
TOLUENE	1294	3	II
TRIETHYLAMINE	1296	3	II
TRIMETHYLCHLOROSILANE	1298	3	II
VINYL ACETATE, STABILIZED	1301	3	II

XYLENES	1307	3	II
ACETONITRILE	1648	3	II
RESIN SOLUTION flammable	1866	3	II
ETHYL ACRYLATE, STABILIZED	1917	3	II
METHYL ACRYLATE STABILIZED	1919	3	II
ALCOHOLS, FLAMMABLE, TOXIC, N.O.S.	1986	3	II
ALCOHOLS, N.O.S.	1987	3	II
ALDEHYDES, N.O.S.	1989	3	II
FLAMMABLE LIQUID, TOXIC, N.O.S.	1992	3	II
FLAMMABLE LIQUID, N.O.S.	1993	3	II
ISOBUTYL ALDEHYDE (ISOBUTYRALDEHYDE)	2045	3	II
DICHLOROPROPENES	2047	3	II
DIISOBUTYLENE, ISOMERIC COMPOUNDS	2050	3	II
TETRAHYDROFURAN	2056	3	II
TRIPROPYLENE	2057	3	II
VALERALDEHYDE	2058	3	II
CYCLOPENTENE	2246	3	II
1,2-DIMETHOXYETHANE	2252	3	II
DIMETHYL-N-PROPYLAMINE	2266	3	II
ETHYLAMINE, AQUEOUS SOLUTION	2270	3	II
ETHYL METHACRYLATE, STABILIZED	2277	3	II
FLAMMABLE LIQUIDS, TOXIC (ISOBUTYRONITRILE)	2284	3	II
METHYLCYCLOHEXANE	2296	3	II
2-METHYLFURAN	2301	3	II
BENZOTRIFLUORIDE	2338	3	II
BROMOPROPANES	2344	3	II
BUTYL NITRITES	2351	3	II
1-HEXENE	2370	3	II
DIETHOXYMETHANE	2373	3	II
DIMETHYL DISULPHIDE	2381	3	II
DIPROPYLAMINE	2383	3	II
FLUOROBENZENE	2387	3	II
METHYL tert-BUTYL ETHER	2398	3	II
PROPIONITRILE	2404	3	II
THIOPHENE	2414	3	II
TRIMETHYL BORATE	2416	3	II
THIOACETIC ACID	2436	3	II
2-METHYL-2-BUTENE	2460	3	II
4-METHYLMORPHOLINE (N-METHYLMORPHOLINE)	2535	3	II
METHYLTETRAHYDROFURAN	2536	3	II
METHYLLALLYL CHLORIDE - CARGO BANNED	2554	3	II
TRIIISOPROPYL BORATE	2616	3	II
AMINES, FLAMMABLE, CORROSIVE, N.O.S	2733	3	II
CORROSIVE LIQUID, TOXIC, N.O.S.	2922	8	II
FLAMMABLE LIQUID, CORROSIVE, N.O.S.	2924	3	II
1,2-BUTYLENE OXIDE, STABILIZED	3022	3	II
1-METHOXY-2-PROPANOL	3092	3	II
ETHERS, N.O.S.	3271	3	II

FLAMMABLE LIQUID, TOXIC, CORROSIVE, N.O.S.	3286	3	II
HYDROCARBONS, LIQUID, N.O.S.	3295	3	II

SECTION 2. Management of security

(1) PEOPLE

Who is ultimately responsible for the management and control of the security plan?

The Managing Director, Mr David Kew

Procedures for recording meetings and actions with regard to security

Security is incorporated within the Business Management System and is included as an agenda item in the regular Business Management System Review meeting which is minuted.

Procedures for receiving and disseminating security information to relevant staff

M&S Logistics IT department is responsible for controlling the external IT service provider to ensure state of the art cyber-security is achieved and maintained. This is backed up by the Company Security Co-ordinator and the Dangerous Goods Safety Adviser who maintain contact with the National Cyber Security Centre and have completed the FORS Counter-Terrorism module, the ACT e-learning course and downloaded the Protect UK app. The Company Cyber-Security Measures & Training Module has been expanded and updated to include details of types of cyber-attack. Security incidents must be registered on the M&S Logistics Incident Report Form.

List of other people responsible for the management of security issues that the security plan applies to, and their duties

See Annex A

List of people authorised to handle high consequence dangerous goods

See Annex B

Security risk assessment matrix UK offices

See Annex C

Risk assessment of the security of HCDG during Handling, Storage and Transport

See Annex D

Details of people who have access to the security plan

See Annex E

Record of reviewing and updating the security plan

See Annex F

Site Plans showing the location of all restricted areas, controlled buildings, protected areas and access points to these areas and buildings, company and visitor parking

See Annex G

Desktop exercises

See Annex H

(2) RESPONSE TO AND REPORTING OF SECURITY THREATS, INCIDENTS AND BREACHES OF SECURITY

Reporting procedures

Security is included in the incident reporting procedure within the Business Management System.

Recording procedures

Incident form is included in the incident reporting procedure within the Business Management System.

Security incident investigation procedure

Investigation of security incidents is included within the Business Management System procedures.

(3) EVACUATION PROCEDURES AND ROUTES

Details of evacuation procedures

As documented in local office fire evacuation plan.

Details of muster points and safe refuge areas

As documented in local office fire evacuation plan

(4) SECURITY OF INFORMATION

Security procedures for hard copy information considered security sensitive

The security plan is not issued as hard copy. Similarly, hard copy information concerning an individual shipment has been eliminated.

Security procedures for electronic information considered security sensitive

The security plan is held electronically on a password-protected computer in a location with restricted access. Access is restricted to staff who need to have it with the information it contains only made available on a need-to-know basis. All documentation for an individual movement is forwarded electronically.

State of the art firewall protects all offices worldwide. Regular meetings and day to day contact with service provider by IT department ensures any new potential security threats are immediately recognised and protected against. A penetration system carries out annual attack on outsourced services and reports weaknesses etc. which enables improvements to be introduced.

How will the records of dangerous goods movements be kept?

Records of all individual dangerous goods movements are maintained electronically.

How will hard copy information be destroyed

By shredding.

5) SECURITY EQUIPMENT

Details of site security equipment

All offices have controlled entry and a monitored alarm system is activated when unoccupied.

Details of maintenance programme for security equipment

Maintenance programme covering the alarm system includes regular servicing

Action to be taken if equipment fails

Maintenance service provider is contacted immediately.

Details of vehicle security equipment

Transport provider responsibility but checked as part of service provider QHSSE auditing programme.

Action to be taken if equipment fails

Transport provider responsibility but checked as part of service provider QHSSE auditing programme.

(6) SECURITY TRAINING

Details of dangerous goods security awareness training programme for all staff

This is based on the Guidance for the Design & Delivery of Security Awareness Training for the carriage of Dangerous Goods by Road & Rail (DfT June 2014).

The following topics are covered:

- The nature of security risks including the types of cyber-attacks
- Recognising security risks including cyber-attacks
- Methods to address and reduce security risks
- Actions to take in the event of a security breach
- Identification of High Consequence Dangerous Goods

Details of security refresher training

Refresher training includes:

- Revisiting the relevant points for each of the above topics
- Any changes to the threat and any incidents which have occurred since the last episode of training
- Cyber-security including the types of attack

Details of training programme for personnel with specific security duties

The Security co-ordinator has attended a Security training course based on the Guidance issued by the DfT on Dangerous Goods Security Training and latest cyber-security requirements delivered by our Security consultant.

Details of procedures for maintaining training records

Individual training records are maintained as part of the Business Management System. All records are maintained electronically for the length of service of each employee. Access to these records is restricted to management.

(7) SECURITY PLAN TEST AND REVIEW PROCEDURE

Details of security drills and testing of the security plan

The security plan is subject to review as part of the BMS review procedure. Similarly, desktop exercises using scenarios such as theft or highjacks and shipment audits are carried out.

(8) DETAILS OF HOW CONSIGNORS, CARRIERS AND/OR DRIVERS WILL BE APPROPRIATELY IDENTIFIED

M&S Logistics will only use approved transport providers who have been subjected to a rigorous audit backed up by spot checks of actual shipments when the opportunity arises.

On arrival at collection point driver must provide a unique collection number to enable shipment to be identified.

(9) DETAILS OF NEW EMPLOYEE VERIFICATION PROCESS

A recruitment procedure exists in the Business Management System and includes an application form and the requirement to obtain references where possible.

SECTION 3. Communication

(1) COMMUNICATION LINKS

Details of communication links with drivers

Transport provider responsibility but checked as part of service provider QHSSE auditing programme.

Details of back-up communication links

Transport provider responsibility but checked as part of service provider QHSSE auditing programme.

Details of vehicle monitoring or tracking

Transport provider responsibility but checked as part of service provider QHSSE auditing programme.

(2) SECURITY ALERTS

People to be informed of a site security alert

David Kew, Managing Director
Regional Director
Ian Ferguson, QHSSE Manager

People to be informed of a journey security alert

David Kew, Managing Director
Regional Director
Site Operations Department
Ian Ferguson, QHSSE Manager

Action to be taken following a security alert

Whoever receives the call must take full details, complete an Incident Form and then pass details to:
David Kew, Managing Director
Regional Director
Ian Ferguson, QHSSE Manager

(3) COOPERATION WITH OTHER PARTIES

Details of how threat information is exchanged with carriers, consignors and consignees and competent authorities

Details passed to local carriers, relevant consignors and consignees and relevant competent authorities. If considered a significant threat, other competent authorities should receive details.

Details of how security information is shared with carriers, consignors, consignees, infrastructure managers and competent authorities

Details passed by e-mail and/or telephone as appropriate to local carriers, relevant consignors, local consignees, local infrastructure managers and local and UK competent authorities.

(4) RESPONSE AGENCIES

Emergency Services 999

Police (CTSA in Great Britain)

Sandbach Police

Tel: 0845 458000
E-mail: ctsa@cheshire.pnn.police.uk

Local authority

Tel: +44 (0) 300 123 5500
E-mail: info@cheshireeast.gov.uk

Billingham CTSA contact

John Bickerstaff
E-mail: John.Bickerstaff@west.yorkshire.police.uk
E-mail : CTSA.supervision@ctpne.police.uk

Local authority

Tel: +44 (0) 1642 393939
E-mail: .customercomments@stockton.gov.uk

Rotterdam Police
Tel: 0900 88 44
E-mail:

Local authority
Tel: 0186 646191
E-mail:

Houston Police (Dial 911 in an emergency)
Tel: +1 281 997 4100
E-mail: jmatherne@ci.pearland.tx.us

Local authority
Tel: +1 281 652 1651
E-mail: ylorfung@ci.pearland.tx.us

Durban Police
Tel: +27 (0) 31 311 2812
E-mail:

Local authority
Tel: +27 (0)31 361 0000
E-mail:

Singapore Police
Tel:
E-mail:

Local authority
Tel:
E-mail:

Department for Transport

Land Transport Security Division
4/28 Great Minster House
33 Horseferry Road
London
SW1P 4DR
Tel: 020 7944 3288

E-mail: landsecurity@dft.gov.uk (Primary Contact)

Highways England

24hr telephone number: 0300 123 5000
E-mail: info@highwaysengland.co.uk

Environment Agency

24hr telephone number: 0800 80 70 60
E-mail: enquiries@environment-agency.co.uk

Subcontracted hauliers

H & P Freightways, Thornaby Depot contact Daniel Raymond - Director

SECTION 4. Measures of site security

(1) DESIGNATED PROTECTED AREAS, BUILDINGS AND LOCATIONS WHERE DANGEROUS GOODS ARE TEMPORARILY STORED IN THE COURSE OF TRANSPORT

Not applicable. Dangerous goods are never stored on M&S Logistics locations.

(2) SECURING RESTRICTED AREAS FROM UNAUTHORISED ACCESS

All offices have controlled access.

(3) PASS SYSTEMS

Not applicable.

(4) MONITORING RESTRICTED AREAS, CONTROLLED BUILDINGS AND AREAS TO PROTECT

All offices are alarmed when not occupied.

(5) SECURITY PATROLS (where applicable)

Not applicable.

(6) VEHICLE/TRAIN/WAGON PROTECTION

Details of equipment fitted to goods vehicles, trains and wagons, or of procedures in place to prevent theft or interference when carrying dangerous goods

Transport provider responsibility but checked as part of service provider QHSEE auditing programme.

Miscellaneous information

All locations involve office operations only. All transport operations are sub-contracted to approved transport providers who have been subjected to a rigorous audit backed up by spot checks of actual shipments when the opportunity arises.

On arrival at the collection point the driver must provide a unique collection number to enable the shipment to be identified.

ANNEX A - List of other people responsible for the management of security issues and their duties

NAME	POSITION	DUTIES
Jaco Gelderblon	Regional Director-Europe	Responsibility for Billingham & Europe
Martin Cockburn	Office Manager-Billingham	Day to day responsibility @Billingham
Kreason Pillay	Regional Director-S Africa, Middle East & India & Asia	Responsibility for S Africa, Middle East & India region
Wim Roldaan	Regional Director-Americas	Responsibility for Americas region
John Harris	DGSA & QHSSE Consultant	Advisory, training and auditing role
Ian Ferguson	QHSSE Manager	Quality, Health, Safety, Security & Environment

ANNEX B - List of people authorised to handle high consequence dangerous goods

David Kew
Martin Cockburn
Jaco Gelderblon
Kreason Pillay
Wim Roldaan

ANNEX C – Security risk assessment matrix UK offices

ASSET		THREAT	VULNERABILITY	RISK IMPACT	INITIAL RISK STATUS	SUMMARY OF COUNTERMEASURES	REVISED RISK STATUS
Vehicles	Tank containers only	Terrorists. Political groups. Former employees of service providers with a grudge.	Significant number of HCDG shipments involved worldwide using approved service providers.	Class 3 (PG II & III) products are mainly involved with potential for fire risk if tank container is involved in a RTA or deliberately emptied and ignited	Medium reflecting transfer of control of approved suppliers to Rotterdam office	Only approved service providers are used with detailed security plans including best practice to ensure regulatory requirements for parking and supervision are always followed	Low reflecting improving control of service providers
Site & Buildings	Sandbach office owned. Billingham office rented.	Low as offices with controlled access only	Low as both offices are secure and alarmed when not occupied.	Low Consequential losses and reduction in new orders.	Low	Controlled access with premises secure and alarmed when not occupied	Low
People	Highly trained and experienced staff	Low with many long serving employees	Low as only approved service providers used	Low Consequential losses and reduction in new orders resulting in potential redundancies.	Low	Robust assessment of new staff supported by subsequent training and regular involvement with management	Low
Road Operation (Journey)	All journeys carried out by approved service providers	Medium as RTAs and parking difficulties can occur.	Medium unless approved service providers are always used	Medium	Medium	Only approved service providers are used	Low reflecting improving control of service providers
Cyber & Information Security	Computer system with up to date cyber-security measures. Hard copy filing system.	Low as information on HCDG only kept in the computer system which is well protected	Low as orders only forwarded to service provider electronically.	Consequential losses and reduction in new orders.	Low	Only approved service providers are used whose computer system has up to date cyber-security measures with electronic transmission of information	Low

Low
Medium
High

Date of risk assessment 18th February 2026

Date of next review February 2027

Assessor: John Harris

ANNEX D - Risk assessment for all offices of the security of HCDG during Handling, Storage & Transport

Assessed by: John Harris	Date of risk assessment: 18 Feb 2026	Date of next review: Feb 2027
---------------------------------	---	--------------------------------------

WHERE	RISK	MITIGATION OF RISK	FURTHER ACTION	Action by whom?	Action by when?	Done	Likelihood	Consequence	Risk Assessment Evaluation Score
All M&S Logistics offices	Cyber-crime	Ensure up to date cyber-security measures provided by approved service providers	Regular contact with approved service provider	IT Manager	Continuous	Yes	1	5	5
All M&S Logistics offices	Insider threat	Pre-employment checks followed by managing through personal security measures	Monitor for any changes in any individual's behaviour	Human Resources Manager	Continuous	Yes	1	4	4
Haulier	Driver not security trained	Only use approved service providers with the required trained drivers	Monitor service provider performance ensuring non-conformances are followed up	Procurement Manager	Continuous	Yes	1	4	4
Haulier	Failure of depot security	Only use approved service providers with best practice depot security	Monitor service provider performance ensuring non-conformances are followed up	Procurement Manager	Continuous	Yes	1	5	5
Haulier	Highjack of loaded vehicle	Only use approved service providers with the required trained drivers	Monitor service provider performance ensuring non-conformances are followed up	Procurement Manager	Continuous	Yes	1	5	5
Haulier	Cyber-Crime	Only use approved service providers with best practice IT cyber-security protection	Regular contact with approved service provider	Procurement Manager	Continuous	Yes	1	4	4
Loading Port	Failure of port security	Only use approved shipping lines calling at ports with known good security provision	Monitor service provider performance ensuring non-conformances are followed up	Procurement Manager	Continuous	Yes	1	5	5
Shipping Line	Use of sub-contract feeder services	Only use approved shipping lines	Monitor shipping line performance ensuring non-conformances are followed up	Operations Managers	Continuous	Yes	1	4	4
Unloading Port	Failure of port security	Only use approved shipping lines calling at ports with known good security provision	Monitor service provider performance ensuring non-conformances are followed up	Operations Managers	Continuous	Yes	1	5	5



ANNEX E - Details of people who have access to the security plan

Senior Management and all operations staff with direct involvement with HCDG shipments.

ANNEX F - Record of when the security plan has been reviewed and tested

DATE	SECTION and/or PAGE	SUMMARY OF AMENDMENTS	SIGNATURE
20.05.10	Page 14	Addition to Billingham products	JFGH
20.10.10	Page 14	Deletion of Maidenhead	JFGH
08.12.10	Page 14	Addition to Billingham products	JFGH
16.04.11	Page 14	Addition to Billingham products	JFGH
28.03.12	Whole document	Addition of Houston office and update of HCDG products carried	JFGH
	Pages 2 – 14	Addition of Security Policy Statement and other minor adjustments	JFGH
17.09.12	Page 14	Addition to Houston products	JFGH
26.06.13	Page 14	Addition to Billingham products	JFGH
27.11.14	Whole document	Addition of Singapore & Durban offices and general update	JFGH
13.05.15	Whole document	Removal of not applicable sections and addition of new HCDG products carried	JFGH
04.11.15	Page 5	Amendment to M&S global office addresses	IF
14.01.16	Page 4	Updating 2016 Security Objectives	IF
17.08.16	Pages 5, 11 & 12	Removal of Ursula van Dyke, addition of Jaco Gelderblon	JFGH
17.01.17	Page 4	Updating 2017 Security Objective	IF
20.01.17	Pages 14-16	Updated list of HCDG	IF
23.03.17	Whole document	Update to reflect revised DfT guidance	JFGH
05.04.17	Annex C	Addition of risk assessments	JFGH
25.01.18	Whole document	Annual update	JFGH
29.03.18	Annex G	Updated list of HCDG	JFGH
14.05.18	Page 6	Addition of e-mail addresses for Shanghai & Dubai	JFGH
31.01.19	Page 4	2019 Security Objective	IF
20.05.19	Annex B	Removal of Rob van Dyke & Steve Shaw	JFGH
20.05.19	Annex G	Updated list of HCDG carried	JFGH
05.01.22	Page 4	2022 Security objective	IF
08.01.22	Whole document	Annual update	JFGH
23.02.22	Whole document	Further improvement to fully comply with latest DfT security guidance	JFGH
04.03.22	Page 14	Updated Police contacts for Billingham	JFGH
		following annual review	
14.07.22	Pages 2, 4, 5, 9, 10, 15 & 16	Introduction of improvements suggested by DfT following audit	JFGH

06.02.23	Page 4	Updating 2023 Security Objective	IF
22.11.23	Whole document	Annual update	JFGH
21.02.24	Pages 2, 3, 10, 14, 16, 17 & 19	Updates and minor improvements	JFGH
12.03.25	Whole document	Annual update	JFGH
26.02.26	Whole document	Annual update	JFGH

ANNEX G - Site Plans

Office site plans are available at each individual office.

ANNEX H - Desktop exercises

SECURITY PLAN DESKTOP EXERCISE 01

If Sandbach office received a telephone call that a HCDG movement had been stolen from a depot, the person who receives the call completes an Incident Report Form M&S 14 Issue:3 and immediately informs the Security coordinator. A check on M&S 14 Issue: 3 in the BMS revealed that this document is actually entitled INCIDENT/ACCIDENT REPORT FORM with no reference to security.

Action 1. JH/IF

- To review whether the word “ACCIDENT” should be removed from the title and text
- To consider simplification of the Form
- To review whether adding of security would be beneficial.

DfT guidance lists various organisations which should be contacted in the event of such a security incidence. These are listed in the M&S Logistics Security Plan. The details listed for the Counter Terrorism Security Adviser (CTSA) for M&S Logistics Billingham office has not been checked by direct contact.

Action 2. JH

- To check email address and telephone number of CTSA contact relevant to Billingham office.

John Harris

3rd March 2022

Action 1.

- The word “ACCIDENT” has been deleted from the Form
- A revised simplified form has been introduced M&S 14 Issue:4
- The word “SECURITY” has not been added to the Form. Comments on security have been added to the M&S claims process however.

Action 2.

- Direct contact with the police has established the name of the **Counter Terrorism Security Adviser (CTSA)** for the area where Billingham office is located and the Security Plan has been updated with this information.

John Harris

SECURITY PLAN DESKTOP EXERCISE 02

Allan Booth Haulage procedures were audited by Ian Ferguson on the 25th February 2026 and found in order. Further desktop auditing has shown however that BMS M&S 07 was last completed in 2020. The question on cyber security introduced in the 2025 issue has not therefore been queried.

Action 1. IF

- Arrange for the latest BMS M&S 07 to be issued to Allan Booth Haulage for completion.

John Harris

26th February 2026