DP WORLD

Policies and Procedures

Group Security Policy

Approved by: Group Chairman & CEO

Department: Group Security

Revision Number: 9.0

Revision Date: March 2019

Table of Contents

1. Introduction

DP World, a leading enabler of global trade and an integral part of the global supply chain, has adopted a common approach to Security and Security management system tailored to the requirements of the entire Group in line with ISO 28000.

DP World's growth strategy is reliant on the continuous identification of threats, risks and vulnerabilities and their mitigation to ensure the protection of all critical resources that support the successful delivery of the DP World strategy.

DP World management recognises that security is a critical function and the ongoing development of an integrated security policy and framework is essential to a common approach to security within the group. The company is committed to embedding Security in the organisational culture, ensuring that a security mindset and security activities become a part of normal working practice.

The DP World Security policy is to be read in conjunction with all **Security Management Principles** and **Security Management Standards**.

2. Purpose

The primary purpose of this policy is to establish the scope, objectives and critical policies that will become the key requirements for Security within DP World.

This policy provides information related to the principles guiding the approach to security implementation and the responsibilities of key stakeholders within the organisation.

3. Scope

The Group Security policy establishes the internal controls and guides stakeholders assigned to deliver security to the group, regions and individual business units. This policy will also outline minimum requirements and standards which are to be adopted across the group.

Ultimately, this policy is the responsibility of the DP World Group Security department and applies to all controlled DP World entities (either through shareholding or management control). Respective business units should also encourage the application of the policy amongst our partners including contractors, suppliers and joint ventures where DP World may be a minority stakeholder.

4. Policy

4.1 Group Security Objectives

The following Group Security objectives have been established and agreed:

- Ensure compliance with all applicable local and international security regulatory and governmental requirements and/or initiatives.
- Identify and evaluate all security related risks and establish controls to communicate, respond, manage and reduce all quantified risks to an acceptable level utilising proactive security risk assessment methods and security risk management programs.
- Monitor and support security projects that enhance the effective delivery of security by adopting innovative security technologies and best practices that have been identified, which will deliver protection of our employees, assets and customers.
- Promote Security awareness with all stakeholders through internal and external education initiatives and communication programs to contribute effectively to the protection of DP Worlds global business interests.

4.2 Group Security Responsibilities

- Review, develop and roll out the DP World Group Security Policy across the group in line with the DP World Group Strategy;
- Establish and implement the Global Security Management System (SMS), to effectively protect the resources and reputation of the group. The SMS will be aligned and accredited with the ISO 28000:2007 certification;
- Monitor the Security Regulatory Compliance of all entities within the Group providing support as required;
- Lead Global SMS Risk Management programs;
- Support and monitor all security projects globally in line with the Group procurement policy;
- Assign Security responsibilities within the group;
- Clearly define the roles and responsibilities of all personnel involved in the global security management system implementation, including review and maintenance requirements;
- Provide support and guidance for the scheduled annual review and update of security management system program activities or following significant organizational change;
- Coordinate and support the planning and execution of security management training and awareness;
- Provide continuous assurance over the security capability through performing audits (internally or externally) on a regular basis to confirm that it is effective and meets stated objectives.
- Provide support for new projects and acquisitions from initial phase.
- Provide support and guidance to Regional office for integration of new businesses/acquisitions.

4.3 Regional Office Responsibilities

- Responsible for the implementation of Security Management System requirements within their region;
- Nominate and assign Security Management System program related responsibilities to a Regional Security Champion;
- Make available the necessary resources to implement and manage the Security Management System;
- Attend and participate in security operational exercises and drills, as required, to raise awareness and validate the procedures documented in the security management system and localised security programs;

- Attend and participate in Security Management Training and Awareness initiatives and remain up to date with related efforts within the respective areas;
- Ensure necessary actions as per the Global Security Management System are undertaken by all BUs under the region in time;
- Ensure transparent and prompt communication with HO is undertaken as per Group Security Communications Protocol.
- Involve Group Security from initial phase for new projects including acquisitions;
- Ensure integration of new projects/businesses in line with Group Security Management Standards.

4.4 Business Unit Responsibilities

- Establish and maintain the Security Management System, adhering to this policy, security management principles, security management standards and all security regulatory requirements;
- Ensure all plans and procedures that have been implemented comply with the ISPS Code and any other relevant compliance and regulatory standards as applicable;
- Undertake Risk Assessment and management in line with the regulatory requirements;
- The business unit must ensure that the security operation is fit for purpose, in that:
    - Personnel must be selected who are suitably qualified and trained;
    - That security information is communicated to all stakeholders in a timely manner, following the Group Security Communications Protocol;
    - That the control measures implemented fulfil the specific requirements for that site and that any changes required in any plans or procedures are thoroughly stress tested and the results are communicated to Group Security for information.
- Establish Key Performance Indicators for measuring the effectiveness of security performance against the security management system;
- The business unit must also monitor the effectiveness of any controls using regular inspections, stress testing, exercises and drills in line with ISPS Code and other regulatory requirements. All KPI's and inspections, testing or exercise must be recorded and communicated for information purposes, with regional heads and well as Group Security;
- Engage regularly with senior management to communicate the performance of the security operation against the established Security Management System;
- Adhere to the wider DP World Sustainability and Environment objectives, to promote a positive impact on the environment. Undertaking low or zero waste programs, ensuring no harm comes to our environment and our people;
- Understand and adhere to the Security Management Principles and Standards as a whole. Any deviation, deliberate or otherwise, must be communicated to the regional heads and well as Group Security, with the justification for separation from the established Security Management System;
- Update information on the Security portal applications as per the requirements of Global Security Management System;
- Provide security awareness for all employees, visitors and stakeholders.

4.5 Security Management Training

DP World aims to raise, enhance and maintain awareness and training to ensure all personnel responsible for security risk management activities are adequately competent and skilled. Individuals assigned to undertake specific roles within the Security group should have the appropriate knowledge and skill set to undertake their assigned tasks. Adequate internal and external training/awareness programs should be established by respective Business Units.

4.6 Policy Compliance

- All DP World entities, should comply with this Policy and the **Group Security Management Principles** and **Security Management Standards**.

- Additional relevant strategies and plans needed to minimize any security risk, should also be developed by the Business Units and communicated to Group Security for information and review. Group Security reserves the right to reject strategies and plans which are not in line with Group Security Principles and would recommend appropriate alternative strategies and plans.

- All security communications should follow the Group Security Communications Protocol, which is available on the Security Connexions Page, under the 'Leadership' tab at:

  https://connexions1.dpworld.com/functions/sp/Pages/default.aspx#?PID=5&1=1

- Each Head of Business Unit will be responsible for implementing the Security Management System, which is necessary to comply with this policy; and will be held accountable for compliance and performance. The Head of Business Unit may delegate individual responsibilities and authorities specified in this policy or associated standards and procedures;

- Group Security will review this Policy and Security Management System annually as recorded on the security profile application, or in the event of a serious security incident that merits an immediate review, requiring remedial action to be taken to maintain its compliance with policy. Additionally, an annual review the associated Security Management Principles and Security Management Standards are to be conducted and any changes, amendments to be communicated to all stakeholders to whom this policy applies.

5. Contact Information

All queries in relation to this policy should be directed to Group Security Department at:

Security.Portal@dpworld.com

6. Related Principles and Standards

The DP World Group Security Policy is supported by the **Security Management System(SMS)**, which in turn is divided into the **Security Management Principles** and the **Security Management Standards**. The security management system defines how security should be applied across the group and is aligned to ISO 28000.

The Policy should be read in conjunction with the below **Security Management Principles** and **Standards**:

Security Management Principles	Security Management Standards
SMP 1 - Security Management System	SMS 1 - Security Policy
SMP 2 - Security Management Control	SMS 2 - Risk Evaluation
SMP 3 - Security Management Operations	SMS 3 - Legal, Regulatory, Statutory and Other Security Requirements
SMP 4 - Security Management Evaluation	SMS 4 - Security Management Objectives
SMP 5 - Security Management Review	SMS 5 - Structure, Authority and Responsibility
SMP 6 - Environment Monitoring and Security Corporate Responsibility	SMS 6 - Implementation and Operation
	SMS 7 - Operational Security Measures
	SMS 8 - Implementation and Operational Security Services
	SMS 9 - Security Documentation and Data Control
	SMS 10 - Security Web Portal Management, Maintenance, Review and Returns

The above Principles and Standards can be found at:

https://connexions1.dpworld.com/functions/sp/Pages/default.aspx#?PID=5&1=1

Or by emailing the Group Security Administrator at: Security.Portal@dpworld.com

Each business unit should seek the support of their respective localised People department, Operations, Commercial, Engineering, Procurement and other departments to provide appropriate support for the effective operation of the Security Management System.

7. Definitions and Terms

In this Policy the following definitions apply, unless the context requires otherwise:

Security Management System	A systemic approach to security management and a critical part for attaining and holding ISO 28000:2007 (see definition below) compliance and certification. The DP World

	Security Management System is compliant and aligned with global security initiatives such as CTPAT, AEO, MEGAPORT etc. (see below).
Security Management Principles (SMP)	There are six security management principles on which operational security system standards are based and the DP World security management system is built on. SMP provides senior management and respective security representatives a framework to guide their business unit towards improved security performance and reduced risk.
Security Management Standards	The security management standards are designed to assist security managers in the development of security management systems linked to security management principles. This includes instructions on the development of security plans, policies, procedures and forms for intrusion protection and guard forces, and a guide to security investigation and performance monitoring.
Group Security Communications Protocol	Defines the method, responsibilities and activities by which communication is conducted and reported across the group.
ISO 28000:2007 Security Management System for the Supply Chain	Is an ISO standard specifying requirements of a security management system particularly dealing with security assurance in the supply chain. A voluntary standard that may enhance overall security of the organisations supply chain.
ISPS (International Ship and Port Facility Security)	is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies. Mandatory across DP World for all maritime terminals and ports.
CTPAT (Customs Trade Partnership Against Terrorism)	Is a voluntary public-private sector partnership program which recognizes that U.S. Customs and Border Protection's (CBP) can provide the highest level of cargo security only through close cooperation with the principle stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers.
AEO (Authorised Economic Operator)	AEO is governed by European Community law and can be defined as an economic operator who is reliable throughout the Community in the context of his customs related operations, and, therefore, is entitled to enjoy benefits throughout the Community.
Security Connexions Page	The primary source for documentation regarding all Security Management System and Policies as mentioned through this Policy. Can be found at the following link: https://connexions1.dpworld.com/functions/sp/Pages/default.aspx#?PID=5&1=1

8. Revision History

Ver.	Date of Changes	Policy Owner	Summary of Changes	Next Review
0.1	July 10, 2006	CEO	Policy review and update	Sept 2007
0.2	Oct 25, 2007	CEO	Policy review and update	
0.3	No Further details as copy of the policy could not be found in our documentation			
0.4	Aug 17, 2010	CEO	Policy review and update	
0.5	Oct 30, 2010	CEO	Policy review and update	
6.0	Feb 13, 2014	COO	Policy review and update	

7.0	Apr 13, 2014	COO	• Template Change • Objective Change	
8.0	Feb 2016	VP – Global Security	• Template Change as per branding • Objective Change	
9.0	Mar, 2019	Group Security	• Template change as per new branding • Policy scope incorporating all divisions of DP World • Objective Change incorporating All divisions of DP World • Policy Objectives made more specific so that it's easier to adopt at BU level. • More details incorporated including responsibilities at Group, Region & BU level.	Mar 2020