DP WORLD

SECURITY POLICY

Introduction

We recognise that security is a critical function and are committed to embedding security in the organisational culture, ensuring that a security mindset and security activities become a part of normal working practice.

Security is fundamental to our operational resilience and commercial integrity. Given our immense geographic diversity, broad range of cultures, and exposure to both natural and man-made threats, embedding a strong, agile, and culturally intelligent security ethos is essential. PNC has adopted a common approach to Security and a Security Management System, tailored to the requirements of the entire company in line with ISO 28000.

Purpose

The primary purpose of the Security Policy is to

- Establish the scope and strategic objectives of the Security function.
- Introduce the critical policies and foundational principles that underpin security activities within our diverse regulatory environments.
- Define and clarify high-level roles, responsibilities, and expectations for all levels of the organization in upholding a proactive and integrated security posture.

Mission

Our mission is to position Security as a critical business enabler by safeguarding people, infrastructure, revenue, integrity, and reputation. We drive resilience and operational continuity through a risk-based, intelligence-led approach that proactively addresses both persistent and emerging threats. Security is not just a function; it is a strategic partner in protecting and advancing our business.

Objectives

Focused on continual improvement of security performance, the following objectives have been established

1. Ensure Regulatory Compliance: Maintain full compliance with international, national, and customer-specific security requirements, such as ISPS Code, ISO 28000, CTPAT, TAPA, etc.
2. Proactively Manage Security Risks: Identify and evaluate all security-related risks within our supply chain and establish controls to manage and reduce all quantified risks to an acceptable level.
3. Enhance Resilience and Preparedness: Ensure security incident management capabilities for all foreseeable scenarios through the development of appropriate plans and scenario-based training.
4. Support Operational Excellence: Monitor and support security projects that enhance delivery by adopting innovative security technologies and best practices to protect employees and assets.
5. Foster a Collaborative Ecosystem: Promote security awareness among all stakeholders through internal and external education initiatives and communication programs.

Policy Compliance

We shall comply with this Policy and the overarching Group Security Management Principles and Security Management Standards. The security team will conduct periodic security reviews, audits, and incident investigations to ensure compliance and continuous improvement. Furthermore, the team will review this policy and the portal management system annually and/or in the event of a serious security incident that merits an immediate review.

Joe.Schofield
Chief Executive Officer
DP WORLD BUSAN
Effective Date : Feb 2026