
DELPHIN BLUE OCEAN B.V.

INFORMATION SECURITY POLICY

Contents

VERSION	
CONTROL.....	3
1. PURPOSE OF THE POLICY.....	4
2. SCOPE.....	4
3. SECURITY PRINCIPLES.....	4
4. DATA PROTECTION AND HANDLING.....	4
5. ACCESS CONTROL.....	5
6. SYSTEM AND NETWORK SECURITY.....	5
7. INCIDENT RESPONSE.....	6
8. SUPPLIER AND THIRD-PARTY SECURITY.....	6
9. EMPLOYEE RESPONSIBILITIES.....	6
10. POLICY REVIEW AND IMPROVEMENTS.....	6

Version Control

Version	Date	Description	Author	Approved By
1.0	November 6, 2025	Document Creation	Compliance Officer or other role	Senior Management 

1. Purpose of the Policy

The purpose of this Information Security Policy is to ensure that all information handled or stored by Delphin Blue Ocean B.V. is protected in a secure and responsible manner. Information security is essential to maintaining trust, safeguarding customer data, and ensuring uninterrupted service availability. This policy outlines the responsibilities, procedures, and controls designed to prevent unauthorized access, data loss, misuse, alteration, or disclosure of information entrusted to the Company.

2. Scope

This Policy applies to all employees, contractors, consultants, and third-party service providers with access to Company systems, data, or operational environments. It covers all platforms, databases, internal documents, communication channels, devices, and software used to support business activities at sporttyp.com.

3. Security Principles

Delphin Blue Ocean B.V. maintains the following core principles of information security:

- **Confidentiality:** Information must only be accessible to authorized individuals.
- **Integrity:** Information must remain accurate, complete, and unaltered except by approved methods.
- **Availability:** Information and systems must remain accessible and functional for operational needs.
- **Accountability:** All personnel handling information are responsible for its correct and lawful use.
- **Regulatory Alignment:** Security measures must comply with applicable laws and operational standards.

4.Data Protection and Handling

Customer data, operational data, and internal documentation must be processed securely at all times.

The Company implements encryption for data at rest and in transit, role-based access restrictions, and strong authentication procedures. Sensitive information must never be stored or transmitted using unapproved personal devices or unsecured communication channels.

5. Access Control

Access to Company systems is provided based on role, responsibility, and job necessity. Access rights are reviewed regularly and updated when individuals join, change roles, or leave the organization. Shared accounts are prohibited, and authentication methods must include secure password protocols and monitoring of login activity.

6. System and Network Security

The Company maintains technical safeguards such as firewall protection, intrusion detection systems, secure software configuration practices, and regular vulnerability assessments. Only approved software and devices may connect to Company systems. All systems must be updated and patched in line with internal maintenance schedules to prevent security risks.

7. Incident Response

If a security breach or suspected threat occurs, it must be reported immediately through internal reporting channels.

The Company will assess the situation, contain the threat, and take corrective measures. Incident reviews ensure lessons learned are applied to improve future preparedness.

8. Supplier and Third-Party Security

Suppliers who handle or manage data or technical services on behalf of the Company must follow equivalent security controls. Third parties may be required to sign confidentiality agreements and demonstrate compliance with data protection standards. The Company monitors and reviews third-party security performance regularly.

9. Employee Responsibilities

All personnel must complete required information security training and follow Company-approved tools and procedures. They must immediately report any suspicious activity, data exposure incidents, or security concerns. Devices must be handled with care, protected with passwords, and kept free of unauthorized software.

10. Policy Review and Improvements

This Policy is reviewed at least once annually, or sooner if operational, technical, or regulatory conditions require updates.

All improvements must follow structured change-control practices to maintain stability and consistency across Company operations.