INFORMATION SECURITY POLICY (ISO27001)

DURO YOKOTA LTD.



INFORMATION SECURITY POLICY (ISO27001)

1.0 PURPOSE OF THE POLICY

The purpose of this policy is to ensure that all information held by Duro Yokota Ltd is protected from loss, misuse, unauthorised access, disclosure, alteration, or destruction. This policy supports our commitment to ISO 27001 and the ongoing management of an effective Information Security Management System (ISMS).

2.0 - SCOPE

This policy applies to:

- All employees.
- All information assets (digital, paper-based, verbal).
- All business systems and processes involving the handling of information.

It covers all business areas including administration, customer data, supplier information, logistics, and IT systems.

3. INFORMATION SECURITY OBJECTIVES

Duro Yokota Ltd is committed to:

- Ensuring **confidentiality:** Information is accessible only to those authorised to access it.
- Ensuring **integrity:** Safeguarding the accuracy and completeness of information.
- Ensuring **availability:** Information is accessible to authorised users when needed.

We aim to:

- Prevent data breaches or unauthorised access.
- Meet the requirements of applicable legislation and regulations (e.g. GDPR).
- Promote security awareness across all staff.
- Maintain business continuity and resilience.

4. RESPONSIBILITIES

- **Management** is responsible for defining, supporting, and reviewing this policy and ensuring appropriate resources are available.
- The **Head of Operations** oversees the ISMS and compliance with ISO 27001.
- **Employees** must comply with this policy and report any security concerns immediately.

5. KEY COMMITMENTS

Duro Yokota Ltd commits to:

- Implement and maintain an ISMS in line with ISO27001.
- Identify and assess information security risks regularly.
- Apply suitable controls to reduce and manage risks.
- Train staff in information security awareness and their responsibilities.
- Monitor compliance and conduct regular internal audits.
- Continuously improve our ISMS.

6. LEGAL AND REGULATORY COMPLIANCE

We will comply with:

- UK General Data Protection Regulation (GDPR).
- Data Protection Act 2018.
- Relevant contractual, legal, and regulatory requirements.

7. BREACH MANAGEMENT

Any actual or suspected breach of information security must be reported immediately to senior management / Directors . All incidents will be investigated, recorded, and corrective actions taken as required.

8. REVIEW AND UPDATES

This policy is reviewed at least annually or following any significant change to the business, technology, or legal landscape.

Signed: D Beaumont

Position: Head of Operations

Date: 30/07/2026 (v. 1.0)

