

Information Security & Data Protection Policy

Policy Statement

At Travel Blue Ltd., we are committed to protecting the personal and business data of our clients, suppliers, and employees. We only collect and use the information necessary for our activities, and we safeguard it through practical and proportional security measures. Our objective is to ensure confidentiality, integrity, and availability of information, while complying with applicable data protection laws (e.g., GDPR).

Key Principles

1. Confidentiality – Only authorized staff can access client and supplier data.
2. Integrity – Data must remain accurate and protected against unauthorized changes.
3. Availability – Data must be available when required for legitimate business purposes.
4. Data Minimization – We collect only the data necessary for our work.
5. Compliance – We respect all applicable data protection laws and client requirements.

Responsibilities

- Management: Ensures systems are secure, provides training, and reviews incidents.
- Employees (all staff): Follow good practices, use passwords, avoid sharing data externally, and report any risks.
- Suppliers: Must comply with confidentiality clauses when handling shared data.

Practical Measures

- Data Storage: All information is kept in secure company systems with password protection.
- Access Control: Information shared strictly on a “need-to-know” basis.
- Data Retention: Unnecessary data is deleted in line with retention rules.
- Backups: Regular backups of business-critical information are maintained.
- Security Updates: All systems are kept updated with antivirus and patches.
- Email Security: Training to identify phishing and prevent leaks.
- Incident Reporting: Any suspected breach is reported immediately to management.



Review

This policy will be reviewed annually to ensure it remains practical, effective, and aligned with Ecovadis requirements.

Effective Date: 01/10/2025

Next Review Date: 01/10/2026