

INFORMATION SECURITY AND CYBERSECURITY POLICY

Our Commitment

At **DLF International Movers**, we recognise that information is one of our most valuable assets. We are committed to protecting information, personal data and the technology systems that support our services through secure, responsible and effective management practices aligned with recognised information security and cybersecurity principles.

The protection of information forms an integral part of our commitment to quality, business continuity, customer privacy and stakeholder trust.

1. Information Protection

We work to ensure the confidentiality, integrity and availability of information by implementing appropriate measures to prevent unauthorised access, loss, alteration or misuse.

Our information management practices are designed to protect both company information and the data entrusted to us by clients, employees, suppliers and partners.

2. Data Protection and Privacy

We process personal data responsibly and in accordance with applicable privacy and data protection legislation.

We implement organisational and technical measures aimed at safeguarding confidentiality and ensuring the secure processing of personal information.

3. Secure Management of Systems and Access

We promote the secure and controlled management of the systems, platforms and digital tools used throughout our operations.

This includes access controls, role-based permissions and the protection of user credentials to reduce risks and safeguard technological resources.

4. Responsible Use of Technology

We encourage the professional, ethical and responsible use of information systems and digital technologies.

All users are expected to contribute to the protection of information and remain vigilant against potential threats, including phishing attempts, fraudulent communications and other suspicious activities.



5. Cybersecurity and Threat Prevention

We work to prevent, detect and mitigate technological risks that may affect our systems, operations or data.

To support this commitment, we maintain appropriate security measures, promote cybersecurity best practices and regularly review our controls in response to evolving threats.

6. Security Incident Management

We encourage the prompt identification and reporting of incidents or vulnerabilities that may affect information or technology systems.

Timely reporting and effective incident management help minimise potential impacts, support corrective action and strengthen our protection capabilities.

7. Training and Awareness

We recognise that security depends not only on technology, but also on people.

For this reason, we promote awareness and training initiatives designed to strengthen knowledge of data protection, cybersecurity and secure digital practices throughout the organisation.

8. Business Continuity and Resilience

We work to ensure the availability of information and the continuity of services through appropriate protection, recovery and risk management measures.

Our objective is to strengthen organisational resilience against technological incidents, disruptions and cyber threats.

9. Compliance and Continuous Improvement

We regularly review our security measures to ensure they remain aligned with technological, regulatory and organisational developments.

Continuous improvement is a fundamental principle in maintaining a secure, reliable and resilient digital environment.

10. Our Objective

To maintain a strong culture of information security and cybersecurity that protects data, supports business continuity and strengthens the trust of clients, employees, suppliers and other stakeholders.

