

# Security Policy

Data security is at the heart of our business and an essential part of the TLScontact culture. We handle large quantities of confidential applicant data on a daily basis and our clients and customers trust us to manage this securely.

We are committed to meeting the highest international standards in terms of information security management, as is demonstrated by our global 27001 certification.

Our security policy consists of the following key elements:



**Ensuring compliance with all applicable security requirements**, from local legislation, client contracts, international standards and group policies.



**Ensuring timely reporting and proper handling of security incidents**, which include but are not limited to security breaches, frauds and faults.



**Protecting information assets from potential risks** to guarantee the confidentiality, integrity and availability of personal data for both customers and employees.



**Conducting due diligence on vendor governance** to make sure that the data shared with third parties are properly handled according to the TLScontact Security Policy.



**Making all staff aware of their roles and responsibilities** and of the importance of their involvement with respect to information security management.



**Driving continual improvement** of the Information Security Management System, based on business changes and expectations from interested parties.



**Carrying out consistent compliance assessments and monitoring** to facilitate the effective implementation of security requirements.