Security Policy

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

We are committed to meeting the highest international standards in information security management, as is demonstrated by our Global ISO27001 Certification. We maintain a strategic focus on continuous improvement through implementation and certification of additional best practices recommended within the ISO 27000 family (e.g.ISO27701, ISO27017, etc.) to further enhance our information security management practices.

Our policy consists of the following key elements:

Compliance with Security Requirements

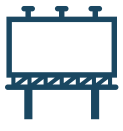
We ensure compliance with all applicable security requirements, from local legislation, client contracts, international standards and group policies.

Incident Management

We establish robust incident management procedures to promptly detect, respond to, and resolve security incidents involving security breaches, service disruptions, fraud and faults.

Protection of Information Assets

We are dedicated to protecting our information assets against potential risks to guarantee the confidentiality, integrity and availability of data for both customers and employees.



Training and Awareness

We commit to providing ongoing training and awareness programs that equip staff with knowledge of security practices and understand the importance of safeguarding information assets.

Roles and Responsibilities

We make all staff aware of their roles and responsibilities to information security management, including specific duties associated with the use of cloud services.

Data Protection Measures

We implement appropriate data protection measures for data stored and processed in cloud and other various environments and systems, including encryption of sensitive data and regular reviews of data access rights to enforce the principle of least privilege.

Compliance Assessments and Monitoring

We conduct regular compliance assessments and monitoring to facilitate the effective implementation of security requirements, including evaluating security posture of cloud service.

Continuous Improvement

We continuously review and improve our information security practices, incorporating lessons learned from incidents and risks assessments, feedback from stakeholders and business needs.