

CORPORATE INFORMATION SECURITY POLICY

October 2026

[intertek.com](https://www.intertek.com)





1. Purpose

Intertek's Corporate Information Security Policy defines the Group's commitment to protecting the confidentiality, integrity, and availability of its information assets. It is established in alignment with ISO27001:2022 standards.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who access, process, store or manage Intertek's information assets.

3. Governance and responsibility

Every employee, contractor and third-party service provider has a responsibility to help protect information security at Intertek. All personnel are expected to protect information assets, comply with security policies, complete mandatory awareness training, promptly report suspected security incidents and support the organisation's information security objectives.

The President of Information Security is directly responsible for managing and maintaining the Information Security Management System (ISMS). The President has the full authority of the Group Executive Committee to plan, implement, and continuously improve the ISMS to ensure compliance with ISO27001:2022 standards.

4. Policy principles

Intertek is committed to:

- Implementing and maintaining effective information security controls to safeguard information assets against unauthorised access, misuse, disclosure, alteration, or destruction.
- Continuously improving its ISMS to address evolving threats and business risks.
- Protecting the confidentiality, integrity, and availability of information throughout its lifecycle.
- Ensure compliance with applicable legal, regulatory, and contractual requirements.
- Promote a culture of security awareness across the organisation.
- Continuously monitoring information security threats, detecting security events, responding promptly to incidents and continually strengthening security controls to address evolving cyber risks.
- Ensuring that all employees, contractors and third parties understand and fulfil their information security responsibilities.
- Ensuring that suppliers and third-party service providers are provided with applicable information security requirements.

5. Supporting policies

The ISMS is supported by a comprehensive framework of policies designed to manage and mitigate risks to information security. These policies include but are not limited to:

- **Acceptable Usage of Technology Policy:** defines appropriate use of company systems and information.
- **Corporate Security Awareness & Training Policy:** manages the delivery and maintenance of security awareness training.
- **Corporate Access Provisioning Policy:** regulates user access to information and systems.
- **Corporate Active Directory Policy:** manages the secure accessibility and management of secure method of logging into corporate resources.



- **Corporate Asset Management Policy:** manages the lifecycle of information assets.
- **Corporate Encryption Policy:** manages secure use of cryptographic techniques.
- **IT Infrastructure Physical Security Policy:** protects physical access to information assets, servers and IT infrastructure.
- **Change Management Policy:** manages the process of planning and coordinating the implementation of all changes and releases.
- **Corporate Incident Response Management Policy:** outlines procedures for identifying and responding to security incidents.
- **Corporate IT System Acquisition, Development and Maintenance Policy:** ensures security considerations throughout the systems development lifecycle process.
- **Disaster Recovery Planning Policy:** ensures resilience and recovery of critical processes.
- **Corporate Data Backup Policy:** defines requirements for data backup and restoration.
- **Corporate IT Third-Party Risk/Vendor Management Policy:** manages risks associated with external suppliers.

All employees, contractors and third-party service providers are expected to comply with these policies, which are available through Intertek's intranet and shared with external parties where relevant.

6. Compliance and review

This policy will be reviewed at least annually or upon significant changes to the organisation or regulatory landscape.

Regular audits, risk assessments, and management reviews will be conducted to ensure ongoing compliance with ISO27001:2022 standards. Non-compliance with this policy may result in disciplinary action.

7. Distribution

Intertek's policies relating to information security are available to all employees through the company's internal intranet.

Authorised by the Group General Counsel and Head of Risk and Compliance, Intertek Group plc.

Name: Todd Andrews

Signed: 

Date: 14 October 2026



8. Version history

8.1 Revision control

VERSION	DATE	NAME	APPROVER	CHANGES
1.0	30.09.2025	Ismail Sidat	Gerrie De Lange	New policy to align with ISO27001.
2.0	14.10.2026	Ismail Sidat	Steven Ramsden, Todd Andrews, André Lacroix	Updated policy to align with best practice.