

Information Security Policy

Integrity Communications Group is committed to maintaining and improving information security within the Group and reducing its exposure to risk. The Group has recognised the need to protect the sensitive data within the business and supplied by our customers. It is therefore group policy to ensure that:

- The confidentiality of corporate, client and customer information will be assured.
- Sensitive information (however stored) will be protected against unauthorised access.
- The integrity of information will be maintained.
- Information will be communicated to all authorised personnel and interested parties.
- The company complies with contractual and applicable regulatory and legislative requirements.
- Business continuity plans for critical activities will be produced, maintained and tested.
- Information security training will be made available to all staff.
- Through the continuous improvement of our Information Security Management System, we will strive to comply with the requirements for ISO27001:2013 Standard and the C&CCC Standard 55.
- The Group will comply to the legal requirements of UK GDPR.
- Information Assets will be Risk Assessed against criteria to determine Risk Acceptance and identify objectives. Risk acceptance will be reviewed and signed off annually.
- Information Security Responsibilities will be defined within the Information Security Management System.

All breaches of information security, actual or suspected will be reported to and investigated by the Information Security Forum Team.

This policy will be reviewed annually to respond to any changes in the Risk Assessment or Risk Treatment plan.



Chief Executive
Integrity Communications Group