

As a trusted partner in the IT services industry, Wavex is committed to maintaining its reputation by providing tools and services to improve efficiency, whilst minimising risks to the confidentiality, integrity and availability of customer and Wavex information and IT systems.

To identify and manage these risks and provide assurance that we are following best practice for information security, we have implemented a combination of technical and operational security initiatives, including establishing an information security management system (ISMS) which is based on international best practice for information security, ISO27001.

The Wavex ISMS has been designed, implemented and operated to achieve the following objectives: -

- Substantiate senior management commitment to protecting customer and Wavex information by maintaining certification to ISO27001:2013.
- Ensure our people have the right skills and qualifications to deliver and support innovative and secure IT solutions.
- Design, develop and manage secure IT solutions which minimise cyber security and operational risks.
- Implement a consistent level of security within all our business activities.
- Comply with legislative and customer requirements for information security.
- Provide information security training to all our staff.
- Identify and minimise risks in our supply chain.
- Protect customer and Wavex information from unnecessary access, modification or loss by identifying and managing risks through the use of policies, processes and controls that are regularly audited.
- Continually review and improve our security.

Signed.

Gavin Russell.

CEO.

Date.

For further information on this policy please contact
Miral Laurie (Wavex ISO)

informationsecurity@wavex.co.uk

Information Security Policy

Information Security Responsibilities.

- The Information Security Officer (ISO) is responsible for the implementation and management of the ISMS, including reporting upon its effectiveness to the CEO.
- The Information Security Forum will over-see the implementation and management of security controls.
- Information Asset / Risk Owners are responsible for identifying and classifying their information and addressing risks.
- Managers at all levels are directly responsible for complying with our information security controls and ensuring adherence by their staff.
- All staff including temporary workers, contractors, and where appropriate, 3rd parties are responsible for complying with our information security policies

Security Management.

- Information assets will be identified, assessed for risk and appropriately protected.
- Risk escalation processes will be implemented.
- Security policies covering IT systems, personnel security, facilities, supply chain assurance, business continuity and the collection, use, sharing, retention and disposal of information will be implemented and adhered to.
- Information security training will be undertaken by all staff, including temporary workers and contractors.
- All actual or suspected breaches of information security will be reported to and investigated by the Information Security Officer.
- Compliance with our ISMS and information security controls will regularly be assessed.