Information Security Policy

The management and staff of GlobalReach are committed to maintaining our reputation for deploying stable, robust, scalable, and future-proof Wi-Fi networks by ensuring that our Wi-Fi software, services and solutions, and operational processes minimise risks to the confidentiality, integrity, and availability of our customers and GlobalReach's information and IT systems.

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

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

- Demonstrate senior management commitment to protecting our customers and GlobalReach information by maintaining certification to ISO27001.
- Deliver stable Wi-Fi solutions which minimise cyber security and operational risks.
- Implement scalable systemised processes that support the Global Reach growth strategy.
- Comply with legislative requirements for information protection.
- Comply with customer requirements for information security.
- Provide information security training to all our staff.
- Identify and minimise risks in our supply chain.
- Protect customer and GlobalReach 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.

All staff and, where appropriate, suppliers are required to comply with the GlobalReach ISMS and supporting policies. Noncompliance may lead to disciplinary action or termination of contracts with suppliers.

Signed

Group Chief Information Security Officer

Date 4th JAN 2024

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 MD.
- 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 with.
- Information security training will be available to 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 to our ISMS and information security controls will regularly assessed.

For further Information on this policy please contact
The Information Security Officer Dr Chris Spencer

chris.spencer@globalreachtech.com