INFORMATION SECURITY POLICY

GlobalReach Technology is committed to maintaining our reputation for deploying stable, robust, scalable, and future-proof wireless services and solutions by ensuring that our products and operational processes minimize risks to the confidentiality, integrity, and availability of our customers and GlobalReach's information and IT systems.

We have implemented a combination of technical and operational security initiatives to identify and manage these risks and provide assurance that we are following best practices for information security. These include an information security management system (ISMS) based on international best practices for information security (IS027001).

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

- Demonstrate senior management commitment to protecting our customers and GlobalReach's information by maintaining certification to IS027001:2022.
- Deliver stable Wi-Fi solutions that minimize cyber security and operational risks.
- Comply with legislative requirements for information protection.
- Comply with customer requirements for information security.
- Provide information security training to all our staff.
- Identify and minimize risks in our supply chain.
- Implement scalable systemized processes that support the GlobalReach growth strategy.
- Protect customers' and GlobalReach's 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.

Information Security Responsibilities

- The Group Chief Information Security Officer (GCISO) is responsible for implementing and managing the ISMS, including reporting on its effectiveness to the Global Management Team (GMT).
- The Information Security Forum oversees 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 their teams adhere to them.
- All staff, including temporary contractors and, where appropriate, third-party workers, are responsible for complying with our information security policies.

Cyber Essentials

In addition, GlobalReach has committed to holding a full Cyber Essentials certification backed by the UK government. Covers five main security control groups: firewalls and routers, software updates and patching, malware protection, access control, and secure configuration.

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, information collection, use sharing, retention, and disposal will be implemented and adhered to.
- Information security training will be available to all staff, including temporary workers and contractors.
- The group's chief information security officer will report and investigate all actual or suspected information security breaches.
- Compliance with our ISMS and information security controls will be regularly assessed.

For further Information on this policy please contact the Group Chief Information Security Officer Dr Chris Spencer (D.Sc.)

Signed: 

Dated: 16th June 2025

Cert: IS 692525