INFORMATION SECURITY POLICY

interTouch

interTouch 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 minimise risks to the confidentiality, integrity and availability of our customers' and interTouch's 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. These include an information security management system (ISMS) based on international best practice for information security (IS027001).

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

- Demonstrate senior management commitment to protecting our customers' and interTouch's information by maintaining, and improving our ISMS.
- Deliver stable Wi-Fi solutions which minimise 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 minimise risks in our supply chain.
- Implement scalable systemised processes that support the interTouch growth strategy.
- Protect customers' and interTouch'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.

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

Information Security Responsibilities

- The Group Chief Information Security Officer (GCISO) is responsible for the implementation and management of the ISMS, including reporting upon its effectiveness to the Global Management Team (GMT).
- The Information Security Team 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 team's adherence.
- All staff including temporary contractors, and where appropriate, third party workers, 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 Group Chief Information Security Officer.
- Compliance to our ISMS and information security controls will be regularly assessed.

Signed: _____

Dated: 25th JAN 2023