Information Security Policy
Wireless Logic Group ISO Policies

November 2024

Information Security Policy

Wireless Logic take Cyber Security and Data Privacy very seriously. We have invested in market leading security technologies to ensure the security of the environments we manage and products that we provision. Such measures include the following:

- Email and web security gateways
- Endpoint detection and response
- Automated security patching
- Mandatory use of MFA
- Encryption of all data
- Vulnerability scanning and independent penetration testing
- Security awareness training and phishing assessments
- Collaboration with the National Cyber Security Centre (NCSC)

Scope

The scope of this Information Security Policy covers the provision of complete M2M/IoT managed services for mobile and satellite wireless networks plus fixed line solutions, encompassing SIM connectivity and intelligent networking which is delivered globally. The Wireless Logic Group is committed to ensuring it meets the legal and legislative requirements for the security and management of information systems and the data that resides within them.

Wireless Logic recognises the importance of achieving good standards of Information Security and the impact this has on the effectiveness of the business. It also recognises the need to continually strive for improvements and shall provide a framework for setting and reviewing objectives and measurable targets.

Information Security Management System (ISMS)

Wireless Logic Group has an established ISMS (Information Security Management System) in place which provides a platform for continual improvement in our operations and procedures. The ISMS is also responsible for providing the high standards for Information Security that is expected by our customers and other interested parties. Wireless Logic Group expects that anyone working for, or on behalf of, will comply with the processes and objectives explained in the ISMS.

The ISMS will be maintained in accordance with ISO 27001:2017.

Wireless Logic Group Policy

- It is the expectation of Wireless Logic Group that:
- Any regulatory and legislative requirements relating to information security are met.
- Awareness of IT security issues will be maintained.
- Ensure any breach of security is identified, investigated and corrective actions implemented to prevent a recurrence.
- Information Security objectives have been defined and measured (where possible).
- Company objectives are monitored through the internal audit process and their effectiveness will be quantified.
- Staff are adequately trained, motivated and competent for the job they are required to do. Any training materials will also be made available to staff upon production.
- Procurement of any IT equipment must be completed through Wireless Logic approved suppliers and introduced to the network by a trained member of the IT team.
- Security incidents must be reported immediately to: security@wirelesslogic.com

Communication Strategy

This policy has been communicated to all staff across the Wireless Logic Group.