POLICY STATEMENT

Maintaining and managing Peak’s ICT data and information processing facilities requires a comprehensive and robust policy. The ISO 27001 Information Security Management System (ISMS) standard process provides Peak with a framework and methodology which enables a focused and structured approach to achieving this.

All policies and procedures outlined in Peak’s Information Security policy must be referred to and adopted by all departments to establish and maintain professional good working practices and procedures for the management of an effective ISMS - vital to counter threats to the availability, integrity and confidentiality of Peak’s data and information.

Vulnerability Scanning:

Vulnerability scans are to be undertaken quarterly by a suitably qualified supplier.

Results of the scans are to be reviewed upon receipt with remediations being completed to the following timelines:

Critical – Remediation process to be commenced within 24 hours
High – Remediation process to be commenced within 72 hours
Medium – Remediation process to be commenced within 7 days
Low – Remediation process to be commenced within 28 days

All remediations are to be completed as soon as is practically possible and within three months.

Penetration Testing:

Penetration tests are to be undertaken annually by a suitably qualified supplier.

Results of the tests are to be reviewed upon receipt with remediations being completed to the following timelines:

Critical – Remediation process to be commenced within 24 hours
High – Remediation process to be commenced within 72 hours
Medium – Remediation process to be commenced within 7 days
Low – Remediation process to be commenced within 28 days

All remediations are to be completed as soon as is practically possible and within three months.

NETWORK SECURITY MANAGEMENT:

The management and security of the data and communications network is critical to ensuring the integrity and security of Peak's systems and data. The following controls must be applied:

- Operational responsibility for networks should, wherever possible, be separated from computer operations activities
- There must be clear responsibilities and procedures for the management of remote equipment and users
- Where appropriate, controls must be put in place to protect data passing over the network e.g. encryption

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption must be used on the network to protect information and data and to prevent information being intercepted.

Acknowledgement: I have read and understood the content of this policy. I am aware of where to find it on the Integrated Management System to ensure I am updated with any amendments to it. I agree to abide by the content of this policy at all times.	
Signature:	Date: