POLICY STATEMENT

Peak Collections is committed to the development and maintenance of an Information Security Management System based upon the International Standard ISO:27001. Peak has developed this ICT Security Policy to:

- Provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements;
- State the responsibilities of staff, partners, contractors and any other individual or organisation having access to Peak ICT systems;
- State management intent to support the goals and principles of security in line with business strategy and objectives.
- Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained.
- Optimise the management of risks, by preventing and minimising the impact of ICT security incidents;
- Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required;
- Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats;
- Ensure ICT information security requirements are regularly communicated to all relevant parties.

AUTHORISED USE:

Access to ICT systems and Information for which Peak is responsible is permitted in support of Peak's areas of business or in connection with a service utilised by Peak. Authorised users are defined as: Peak employees, authorised contractors, temporary staff or partner organisations when using information services provided by Peak.

ACCEPTABLE USE:

All users of ICT systems and information for which Peak is responsible must agree to, and abide by, the terms of Peak's Acceptable Use Policy, associated security policies and applicable Codes of Connection or Conduct.

SECURITY AWARENESS:

Peak Collections is committed to promoting safe working practices. All employees will receive security awareness training commensurate with the classification of information and systems to which they have access. Staff working in specialised roles will receive appropriate training relevant to their role. Relevant information security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of information security policies and procedures.

BUSINESS CONTINUITY:

Peak Collections has developed, and maintains, a Business Continuity Strategy based on specific risk assessment to maintain critical business functions in the event of any significant disruption to services or facilities on which Peak is reliant.

MONITORING AND REPORTING:

Peak reserves the right to monitor the use of ICT systems and information, including email and internet usage, to protect the confidentiality, integrity and availability of Peak's information assets and ensure compliance with Peak's policies. Peak Collections may, at its discretion, or where required by law, report security incidents to the relevant UK authorities for further investigation. As part of the standard audit review process, Internal Audit will routinely assess compliance with Peak's ICT Security Policy and applicable ISO27001 controls and report matters to senior management where appropriate. Security incidents reported through the Security Incident Management Policy and Procedures, will inform on the effectiveness of ISO27001 controls and assist in identifying training and awareness requirements and improvements through the Improvement procedure.

RISK ASSESSMENT:

Peak Collections has developed a Risk Management Strategy and the risk to Peak's ICT systems and information will be managed under this framework with reference to the guidelines detailed in **BS 7799-3:2006 Information security management systems – Part 3**: Guidelines for information security risk management. Reviews are independent, unbiased and verified by either internal audit or external parties when required.

SECURITY POLICY REVIEW:

Peak Collections will conduct an annual review of the policy or following any significant security incidents, changes to UK or EU legislation or changes to Peak's business requirement or structure.

ASSET MANAGEMENT:

Peak will maintain an inventory consisting of all information assets which will be managed in accordance with Peak's information security policies and procedures.

SANCTIONS:

Failure of Peak employees to comply with Peak's Information Security Policy may lead to disciplinary action under Peak's disciplinary procedure.
Failure of contractors, temporary staff, partners or third party organisations to comply with Peak's Information Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

COMPLIANCE WITH LEGAL AND CONTRACTUAL OBLIGATIONS:

Peak Collections will abide by all UK legislation relating to information storage and processing including:

- The Data Protection Act (2018)
- GDPR
- The Freedom of Information Act (2000)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)

Peak will also comply with any contractual requirements, standards and principles required to maintain the business functions of Peak including:

- Protection of intellectual property rights;
- Protection of Peak's records;
- Compliance checking and audit procedures;
- Prevention of facilities misuse;
- Relevant codes of connection to third party networks and services.

RESPONSIBILITIES:

Co-ordination: Peak Collections co-ordinates information security management across the company network via the IT Department.

Security Officer: Peak's Information Security Manager (OCS – Oscar Compliance Services) is responsible for ensuring policies and procedures are in place to cover all aspects of ICT systems and Information security. All policies will be communicated across Peak to ensure good working practices and to minimise the risk to Peak's reputation.

Directors: are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with Peak's ICT Security Policy. Day to day responsibility for the management of ICT systems and information may be delegated to staff designated as information or system owners within departments.

Users of resources: It is the responsibility of any individual or organisation having access to Peak's ICT systems and information to comply with Peak's ICT Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the ICT systems and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the Security/Business Continuity Manager via Peak's Incident Reporting system.

DEVELOPMENT OF SPECIFIC ICT POLICIES, PROCEDURES AND GUIDELINES:

Peak Collections is committed to the ongoing development and review of ICT policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. This work will be co-ordinated by the IT Manager. A list of current supporting documents is included in Appendices A-B. New policies and procedures are distributed to all stakeholders at the time of issue. Appendices A-B of this policy are updated during the annual ICT Security review.

BREACHES OF POLICY:

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Peak assets, or an event which is in breach of Peak security procedures and policies.
All Peak employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through Peak Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of Peak.

Peak Collections will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

INCIDENT REPORTING:

Breaches can involve not only Information Technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern or which may contravene Peak associated policies.

INCIDENT MANAGEMENT:

During reporting of a breach, details of the incident will be entered into the logging system - either by the person directly reporting the incident or by the Information Security Manager. The Information Security Manager will then determine if the incident needs to be escalated to the appropriate authorities and clients.

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: