Information Security Policy

Objective and Scope

The objective of the Prevision Research Information Security Policy is to ensure the company ISMS is in place to ensure the integrity, security and availability of data and information required to conduct business is never put at risk.

This policy takes into account business risk, regulatory obligations and risks and vulnerabilities in relation to information security.

This policy is owned by the Operations Director, approved by senior management and applies to all users of the ISMS, including those who develop, maintain, monitor and continually improve data and information security.

Information Security Objectives

Information security at Prevision Research means the secure knowledge held at Prevision Research is protected from unauthorised use of business sensitive and personally identifiable information, including all forms of electronic data.

Information security objectives apply to personal information and business-sensitive information when collected, held, used and stored for legitimate business purposes. Refer to Document 'Leadership and Commitment' for the suite of objectives.

Refer: Monitoring, Measurement and Analysis policy and Plan

The information security objectives::

- Threats and vulnerabilities risk management:

  Our objective is to protect information and information assets against threats and vulnerabilities, to which Prevision Research may be exposed

- Privacy protection

  Confidentiality involves restricting data only to those who need access to it. Encryption and setting passwords are ways to ensure confidentiality security measures are met.

- Data Integrity

  Data protection is making sure data in the possession of Prevision Research is accurate, reliable and secured against unauthorised changes, tampering, destruction or loss.

- Data Availability

  Private information is readily available for anyone who is authorised to access it, as and when a customer requests to view their profile.

Assets included in these objectives are:

- information assets such as databases, software applications and systems,
- Hardware assets including desktop computers and laptops, communications equipment and telephonic devices, and

Information Security Policy

- Public facing applications and websites intended to be accessed by external parties. Roles, Responsibilities and Authorities

Roles and responsibilities for the information security ISMS are assigned to the:

- Centre Manager,
- Operations Director, and
- Managing Director.

These roles shall jointly share responsibility for providing an ISMS in compliance with ISO 27001.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Policy	5.2		5.2	5.1

Related Information

- ISMS Framework and supporting procedures
- Monitoring and testing program, including penetration testing

Information Security Policy

Policy

Prevision Research applies a consistent, risk-based approach to information security that maintains the confidentiality, integrity and availability of information. It does this by protecting information against unauthorised disclosure, access or use, loss or compromise (malicious or accidental), or a breach of privacy. This includes identifying and managing risks to information, applications and technologies throughout their lifecycle by implementing and maintaining an ISMS in compliance with the ISO 27001.

Risk assessment

Prevision Research applies risk-based thinking to the ISMS by undertaking risk assessments of the ISMS and supporting procedures and information systems.

The risk assessment process identifies potential vulnerabilities and allows security control measures to be implemented, therefore potentially reducing and maintaining the identified risk to an acceptable level.

Access management

Designated users shall be provided access to the Prevision Research information systems by the Operations Director only after approval from the relevant line manager or delegate. Access is afforded according to the individual's role and responsibilities within the organisation and monitored in accordance with Prevision Research policy.

Only the Operations Director with high-level access rights are afforded Privileged User status.

Contractor and third-party access is permitted only if agreed to by the Operations Director .

Asset security management

The Operations Director will be responsible for the implementation and management of all information systems.

Server storage and backup of information systems are auto backed up according to a controlled schedule with frequency determined by information criticality and risk.

Backups of business critical data are tested to ensure full system recovery functionality. The restoration process is documented and tested annually. Backup media standards require media retrievability within 48 hours.

Business continuity and disaster recovery

Business Continuity and Disaster Recovery Plans are in place and tested for all critical information systems. Testing frequency is dependent on the criticality of the information systems as nominated by the Operations Director. Testing measures the ability to recover the system within agreed timeframes.

Physical security

Access to secure areas where network equipment is operational is restricted to Operations Director and nominated senior personnel.

Information Security Policy

Software applications security

Software applications used for operating information installed on, or stored on Prevision Research computer systems shall be subject to licensing requirements. Software applications including patches, upgrades or new versions, shall be tested, securely stored and documented before being uploaded into any live information system.

Operational software shall be maintained at current versions.

Information classification, labelling, handling and distribution

Information assets are classified into four categories:

1. Public
2. Business Use Only
3. Confidential
4. Highly Confidential.

Each information asset shall have a nominated owner who is responsible for classifying, labelling , handling and distributing the information asset according to its classification status.

Information security incident notification and reporting

A security incident is defined as any action or event in breach of this Information Security Policy or any other information security related policy or instruction referred to in the ISMS framework document.

As soon as an incident or suspected incident is reported, the Operations Director shall carry out an immediate technical investigation or evaluation to determine the extent of the incident or breach and the resultant impact to Prevision Research. A full investigation, remedial action and report shall be submitted to the Managing Director, dependent upon the outcome of the investigation.

Prevision Research considers any breach of security to be a serious offence and reserves the right to act in the best interests of the organisation.

Awareness and communication

Aspects of information security, including confidentiality, privacy and policies relating to the ISMS are included in staff or vendor induction.

This policy shall be made available internally, externally to any interested party and displayed publicly.

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from management reviews, regulatory changes and audits. Changes to the policy must be approved by a senior executive then communicated to all previous persons or organisations with access to the policy. Refer below for the most recent review.

Information Security Policy

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N