Document number: OC.12
Document Name: Infosec in Project Management Policy
Document Owner: Operations Director
Issue Date: 01/05/2024
Current Revision Date: 01/05/2024

prevision research
THE DATA COLLECTION EXPERTS

Infosec in Project Management Policy

Objective and Scope

The objective of this Policy is to ensure information security is fully integrated into project management.

Information security risks related to a project are identified, known and actioned as part of the overall project management lifecycle.

Roles, Responsibilities and Authorities

Roles and responsibilities for this policy are the responsibility of the project manager who shall appoint a competent person within the project team to take ownership of information security risk management.

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 Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
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**
Infosec in Project Management Policy		6.1.5		5.8
Information security requirements analysis and specification		14.1.1		

Related Information

- Information Security Policy
- Threat Intelligence Policy

Policy

Prevision Research shall ensure known or suspected risks pertinent to a project are relayed to the nominated project information security risk owner. This applies to any type of project regardless of complexity, duration, size, discipline or application.

The project manager shall follow through to ensure related infosecurity risks and deliverables are effectively addressed throughout the life of the project, including the specified infosecurity technical specifications for the project.

Infosec in Project Management Policy

Any lessons learnt from the project shall be shared with the threat intelligence nominated personnel and ISMS representative, IT Representative and Privacy Officer accordingly.

IS lifecycle integration

Project planning

- Scope and requirements of information security of a project are determined and documented including:
  - the information risk classification of the project and its data content
  - Infosecurity technical specification for the project to ensure IS standards are met and where practical, represent IS improvements.
- Known or suspected information security risks are identified at the planning stages in relation to the internal and external project information specification and requirements.

Project in progress

- Throughout the life of the project the known and anticipated risks and controls continue to be risk reviewed to ensure they continue to meet the needs and specifications of the project.
- Any third party working on the project shall be informed of the information security requirements of the project and any work undertaken shall be supervised to ensure compliance is achieved.
- Specialist expertise may be sourced at any time to ensure risk treatment is adequate against project specification and governance requirements.
- As the project progresses key IS performance measures and treatments (both internal and external) are tested and approved as required by the project plan before progressing to the next phase.

Project completion

On project completion:

- An audit of legal, statutory and regulatory compliance shall be completed.
- An independent review of the contract specification in relation to information security shall be undertaken and compliance confirmed.
- Measure of enhanced or upgraded ITS infrastructure.
- Findings and lessons learnt from the project shall be shared with interested parties including other projects and those involved in threat intelligence activities.

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 infosec groups, regulatory groups 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.

Infosec in Project Management Policy

History table

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