Organisational Roles, Responsibilities and Authorities Policy

Objective and Scope

Roles, responsibilities and authorities define the duties of an individual in the context of what their workplace roles are, and what they are expected to achieve.

The objective of this policy is to document Prevision Research assignment of responsibilities and authorities for relevant roles in the management of information security systems.

The scope of this policy includes the identification of the information security critical roles and subsequent assignment of responsibilities and authorities.

Roles, Responsibilities and Authorities

The Managing Director undertakes to manage the provision of staffing and other specialist resources associated with information security related roles, and the assignment of responsibilities and authorities afforded to each role.

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
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
Employment Act 2002	https://www.legislation.gov.uk/ukpga/2002/22/contents
Health and Safety at Work Act 1974	https://www.hse.gov.uk/legislation/hswa.htm
Equality Act 2010	https://www.legislation.gov.uk/ukpga/2010/15/contents
Modern Slavery Act 2015	https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted
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**
Organisational roles, responsibilities and authorities	5.3	6.1.1	7.1	5.2
Segregation of duties		6.1.2		5.3
Management		7.2.1		5.4

Organisational Roles, Responsibilities and Authorities Policy

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**
responsibilities				
Management direction for information security		5.1		5.2
Contact with Authorities		7.0		5.5
Contact with special interest groups		6.1.4		5.6

Related Information

- Staff development
- Position Agreements or Position Descriptions
- Employment Contracts or Agreements
- Confidentiality Agreements – included in induction paperwork
- Disciplinary process documentation

Policy

Senior management shall ensure responsibilities and authorities are assigned for ensuring all facets relating to the information security management system, internal ISMS systems and reporting of IS performance conforms to requirements as stated in company policies, procedures and prescribed in ISO 27001: 2022.

ISMS Representative - Conformance to ISO 27001: 2022

Conformance to ISO 27001: 2022 means conformance by the Prevision Research certification to ISO 27001 is achieved and maintained.

Role

The Role of the ISMS Representative is documented in a Position Description.

The ISMS Representative role works closely with the Operations Director in risk assessing, developing, implementing and controlling the information and information systems that comprise the ISMS.

Responsibilities

1. Deliver and maintain a risk-based ISMS Framework.
2. Monitor and measure performance of the ISMS across the jurisdiction using a performance monitoring and measurement PMMP program jointly with the IT team and DPO.

3. Keep senior management and interested parties informed to ensure shared responsibilities by all parties.

4. Performance reporting and management review is undertaken.

Authorities

Business management takes accountability for the provision of infrastructure and resources, technologies and other assets, competency and training provisions and any other IT needs necessary to comply with the legislation. The ISMS Representative is authorised to ensure resources are made available and are fit for purpose within the authorised budget.

Data Privacy/Protection Officer - Assigned Role for data privacy/protection (Confidentiality, Integrity and Availability)

Role

The Role of the Data Privacy Officer is documented in a Position Description.

The Protection Officer, ISMS Representative role and the Managing Director work closely in risk assessing, developing, implementing and controlling the information and information systems that comprise the ISMS.

Should there appear to be or is a conflict of interest between the DPO role and that of other roles the DPO may hold in the organisation, the DPO shall consult with the ISMS Representative and the Managing Director. A joint decision making process shall be undertaken to reach consensus or alternatively, an independent advisor shall be sourced.

Responsibilities

The primary role of the Data Privacy/Protection Officer (DPO) is to ensure that the organisation processes personally identifiable data of any individual (data subject) in compliance with the applicable data protection rules.

This role has clearly stated regulatory duties in relation with privacy legislation such as GDPR - DPO roles.

The DPO receives support from the ISMS Representative and IT Representative and reports directly to the most senior level management.

Authorities

This role has clearly stated authorities afforded it in relation with privacy legislation such as GDPR - DPO roles.

The Prevision Research shall provide the resources and involve the DPO in a timely manner and ensure the DPO has the authority to undertake the role.

Policy Owner - Assigned Role for policy development and review

Role

Policy development ownership is assigned to a senior management role or roles with the skills to:

- determine policy need
- identity and interpret legal and regulatory requirements associated with the policy content
- engage in consultation with interested parties regarding policy content
- document the policy for review and approval by an executive representative

Responsibilities

The assigned management representative takes responsibility for collaboration with leadership and the policy development lifecycle:

- Planning
- Development to draft
- Review and approval
- Implementation and roll out
- Measurement of effectiveness of the policy post implementation

Authorities

Policy developers require the authority to initiate development and follow through the policy lifecycle including mandating training needs, a roll out plan, monitoring policy effectiveness through setting and measuring KPIs.

The level of authority required to complete the policy lifecycle is separate from the authority normally afforded a working role within the organisation and lasts until the policy is finally embedded within the organisation.

Project Manager Role

Role

As part of the general project management process, a project manager role shall be established to manage and oversee a project from inception to completion to ensure it is integrated into the information security business systems.

This role is assigned to persons with the knowledge, experience and capability required for the particular project and in particular, IS objective and project IS specific risks as they relate to the project work. This may vary from project to project.

Responsibilities

The responsibilities of a Project Manager shall be documented in the scope of the project with assigned responsibilities and authorities at each stage of a project lifecycle.

As a minimum, Project Managers shall have a working knowledge of the IS risk assessment process and IS related project objectives in line with corporate IS objectives.

Delegated responsibilities may be assigned to an individual (2IC) when a Project Manager is not available.

Organisational Roles, Responsibilities and Authorities Policy

Authorities

Project Manager IS authorisations and access rights shall be assigned to allow effective access to allow decision making and project progress to proceed uninhibited by lack of IS authorisation. This generally involves access to information systems appropriate to project needs and ability to effectively allocate resources to the project. The role must have limitations of access to core secure data according to the Head IT approval for security purposes.

Special Interest Group Representative - Assigned Roles for contact with authorities and special interest groups

Role

Contact with authorities includes privacy and information security regulators, government and local government agencies, law enforcement agencies and local law agencies in circumstances where a breach involving information security systems or privacy of information occurs. This also extends to non regulatory bodies such as product suppliers or essential services when a breach or suspected attack involving email/internet, devices or other like systems is suspected.

Responsibilities

Contact with authorities shall be assigned to the following roles:

- In the case of an immediate known emergency every individual has an obligation to make contact with the relevant provider as soon as possible and then contact the internal delegated role as prescribed in emergency planning documents.
- Planned contact of suppliers of software applications and other IT providers made on a regular basis by the nominated IT representative for the purposes of staying up to date with current issues and future planning.   The Operations Director shall assign these roles. Contact may be in the form of a user group, updates from websites or joining forums. This is the choice of the nominated individual.
- Membership of information security and like professional associations and groups is encouraged and supported as part of overall staff development. This includes opportunities for knowledge updates, new product reviews, early IS alert warnings and vulnerability updates.

Authorities

Whilst there is no limit on staff participating in membership and informative groups, the Operations Director must be kept informed of memberships and staff may be required to sign an NDA at the discretion of the Operations Director in relation to sharing Prevision Research sensitive information.

High risk segregation of duties within Information Security - Assigning Authorisations

Segregation of Duties (SoD) refers to practices where the knowledge and/or privileges needed to complete a process are broken up and shared among multiple authorised users so that no single individual is capable of performing or controlling an information system.

Organisational Roles, Responsibilities and Authorities Policy

Assigning authorisations is the domain of Head IT or an independent IT professional appointed by the Board of Directors.

Applies to every role with duties working within the information systems architecture

When assigning duties the following mandatory protocols shall be initiated and tested by independent audit:

Mandatory control 1:

No single person within the organisation is afforded authority over an end to end system nor more then one functional area such as operations, development or testing.

Mandatory control 2:

Clear and unambiguous levels of responsibilities shall be assigned and limited to individuals in such a way as to mandate checks and balances within the system and minimise the opportunity for unauthorised access and fraud.

Mandatory control 3:

Separation of duties between operations, development and testing of security shall be assigned to different individuals with different skill sets. This is subject to independent audit.

Responsibilities

Responsibilities must be assigned to individuals in such a way as to mandate checks and balances within the system and minimize the opportunity for unauthorized access and fraud.

A senior independent individual (Centre Manager) not working within the IT sphere, shall take responsibility for receiving reports from individuals from operations, development and testing departments, then collate and independently report both to the Managing Director plus an independent audit role for scrutiny.

Authorities

Where practical, assign a third party to monitor security, conduct surprise security audits and security testing. The third party shall report directly to the Operations Director.

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.

Organisational Roles, Responsibilities and Authorities Policy

History table

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