Human Resources IS Employment Policy

Objective and Scope

The objective of this policy is to document how Prevision Research shall manage the human resources provisions required for the establishment, implementation, maintenance and continual improvement of information security and the support of the information security system.

The scope of this policy includes competency provisions of all personnel, regardless of their employment arrangement, throughout their employment lifecycle.

Roles, Responsibilities and Authorities

The Centre Manager or competent delegate takes ownership of the provision of resources, including employment lifecycle and staff development.

A designated IT officer shall be nominated by the Operations Director to ensure the interests of information security are considered and enabled in all aspects of employment and competency.

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
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.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
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/

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**
Resources	7.0		7.1	
Screening		7.1.1		6.1
Terms and conditions of employment		7.1.2		6.2
Prior to employment - management responsibilities		7.2.1		5.4
Confidentiality and Non-disclosure Agreements NDA		7.1.2		6.6
During employment		7.2	7.2/3	

Human Resources IS Employment 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**
IS Awareness		7.2.2	7.2/3	6.3
Disciplinary process		7.2.3		6.4
Termination / change of employment		7.3 /7.3.1		6.5

Related Information

- Training Matrix
- Position Agreements or Position Descriptions
- Employment Contracts or Agreements
- Confidentiality Agreements (NDA)
- Disciplinary process documentation

Policy

Information security employment lifecycle obligations at Prevision Research commence at the resources planning stage and continue throughout the employee working life until end of employment. Regardless of the employment or engagement arrangement, Prevision Research shall ensure each individual person understands their role and responsibilities for information security.

Resources - employment lifecycle

Prior to employment or appointment

Screening at selection and appointment

- As part of the general employment process, pre-employment background checks are undertaken using employment and/or character references, CV checks, police checks if/where required by law (working with children/vulnerable persons), qualification or professional standing verifications and ID validation.
- When roles are highly information security sensitive (access to source data or mass personal information data) additional screening checks including a police check is required.
- If verification cannot be completed in a timely manner, a risk review shall be undertaken to determine what if any mitigation measures shall be undertaken or absolved with risk acceptance. At sometime when appropriate the background checks must be completed, reviewed and actioned accordingly.
- Records and evaluation of potential candidates shall be kept according to employment regulations.

Terms and conditions of employment

Human Resources IS Employment Policy

- Employment and/or contract agreements shall include the roles, responsibilities, accountabilities and obligations for information security and the handling of personal information. The agreement should be clear and concise in stating employer and employer obligations for information security.
- Individuals with access to personal data or business sensitive information (as per Information Classification Policy) are required to sign a Non-Disclosure Agreement NDA.

Confidentiality and non-disclosure agreements NDA

Based on the employment terms in the agreements, a Confidentiality or Non disclosure agreement NDA shall be agreed between the company and the individual person. The NDA shall include:

- Identification of confidential information included in the NDA
- Duration of the agreement
- Responsibilities of all parties including permitted use
- Actions if a breach of the NDA occurs

During employment

Information security induction and awareness is undertaken at commencement of employment and periodically throughout employment. This is based on the assigned role of the individual and their access to personal and business sensitive information as defined in the Information Classification Policy.

As part of the Prevision Research staff development and performance review programs, further training needs shall be identified and provided.

Termination or change of employment

Disciplinary process for IS breach

An investigation shall commence when it is known that an IS breach has occurred. The disciplinary process is the standard business investigation process with the exception that an IT competent person and/or the Data Privacy Officer may be added to the investigation team as deemed necessary to reach a fair conclusion.

As a result of the outcome, the company disciplinary process may be enacted.

Change of employment

When a change of employment status occurs that involves duties and responsibilities, a review of the role of the individual's IS access classification shall be undertaken to determine the need for changes to PI data access controls. This may also generate additional training needs.

Termination of employment

When an individual ceases to work for the organisation, the information security and legal responsibilities that remain with the individual according to their role and employment agreement shall be documented in the termination correspondence.

At time of termination, an agreement regarding business related data content of mobile devices owned by the individual shall be agreed to protect the interests of the company.

An IT representative shall initiate cleansing of devices of PII and business sensitive information according to the role.

Human Resources IS Employment Policy

Workforce (Information Security) competence, awareness and training

The Prevision Research workforce competence program forms part of the business resources planning.

Employed persons are provided access to and made aware of their obligations to the following policies:

- All individuals - Privacy, Information Security, Social Media, Asset Management, Media Handling, Remote and Teleworking, Mobile Devices, Building/Infrastructure Security and Clear Desk/Clear Screen
- Plus for high ITC security access - Cryptography Compliance (ITS), Communications (Network) Security, Software (Applications Assets) Management and IT Operating Systems Security

Ongoing employment and training

- Refresher ITC training is undertaken annually, when changes to policies or procedures occur and when the role of an individual changes.
- Competency needs of individuals shall be reviewed annually to confirm and deliver competency needs.
- When a role changes a performance review of training and competency needs shall be undertaken and actioned accordingly.

Records of training and development shall be retained.

Communication (Information Security)

Communicating information security content or material internally and externally is based on:

- What to communicate?
  Determining by roles ‘whether’ and ‘what’ information needs to be communicated based on a need to know basis.
- Who to communicate with?
  Internal roles of individuals in the organisation that will be impacted by the information.
  External needs of stakeholders who have an interest in the information content.
- When to communicate?
  Timeliness and timelines associated based on the information content.
- How to communicate?
  The most effective and secure method of communication including secure access controlled delivery, social network public delivery, internal email and public website.
- Who approves the communication?
  The owner of the information shall determine what/who/when/how the information is communicated and whether senior management approval is required to give the ‘go ahead’.

Disciplinary process

A disciplinary process is in place and communicated at induction. Refer Disciplinary Action Procedure.

Human Resources IS Employment Policy

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change failure or a policy breach is known to have occurred. Refer below for the most recent review.

Human Resources IS Employment Policy

History table

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