Human Resources Policy

Objective and Scope

The objective of this document is to establish employment lifecycle standards and protocols.

The scope of this document covers employment arrangements and some contract positions related to suppliers with information security access.

Roles, Responsibilities and Authorities

The Operations Director shall identify resources needs and provision of resources to appoint and employ personnel.

The Centre Manager shall take responsibility for recruitment and employment lifecycle through to termination.

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**
Support - Resources	7.1		7.1	6.1 l 6.2 l 6.4 l 6.5

Related Information

- Employment agreements
- Position descriptions
- Confidentiality l Non-disclosure agreements
- Remote working - working from home
- Disciplinary process
- Employee Training/Staff Development Plan

Human Resources Policy

Employment commencement

Prevision Research shall manage human resources whether employed or contracted, in a manner that does not

compromise the information security confidentiality, integrity and availability CIA of personnel.

Application Reviews - Background screening

1. Background checks are undertaken of prospective employees (short listed applicants) against police records, immigration work related status , previous employment history against applicants claims. Where relevant to the intended role, other legal checks may be applied.
2. Reference checks - personal and business or educational/academic status claims as applicable.
3. Personal identification via passport l drivers license or other as issued by specific regulators
4. High risk classification roles - Further detailed review such as interview or feedback from previous employer.
5. Police clearance required for high risk IT roles

Specific IT roles

When the advertised role is an IT specific role, a competency assessment at interview stage, confirmation of competency from a previous employer or significant recent upgrading of competencies is considered a risk averse measure.

Employment Policy - Employment or contract agreement (terms and conditions)

The employment or contract agreement shall document both the employees or individual and employers obligations and responsibilities for their role and specifically for information security. Where a probationary period applies (to employees or contractors), this shall be noted in the employment or contract agreement.

The following shall form part of the employment or contract agreement:

1. Non-disclosure agreement / statement NDA.
2. CIA Confidentiality agreement (may be integrated with NDA).
3. Legal responsibilities and rights including copyright, privacy breach reporting, working with children and others according to jurisdictional laws.
4. Jurisdictional scope of the role including remote working arrangements.
5. Responsibilities for access to and use of assets and their classification level, information processing facilities and information handling services (internal and from interested parties).
6. Procedures to be enacted in the case of a breach of ISMS or CIA.
7. Asset ownership and CIA clearance arrangements on termination of employment or contract.

Human Resources Policy

Onboarding period - probationary period

Onboarding commences on formal acceptance of appointment. Where job acceptance has occurred however formal documentation of appointment is still pending, onboarding should still commence without exposing the company to CIA risk through provision of administrator or other high risk access.

Onboarding shall include:

- Induction into the organisation and its ICT systems
- Provision and awareness of ICT policies including password management
- Issuance of assets and access to assets
- Remote working information security arrangements - may involve a risk assessment of the remote location (home office)

A probationary period of no longer than 90 days may be applied where particular skills and competencies are critical to the role. Probationary periods will be identified and agreed, if applied, as part of the employment agreement.

Conditions and expectations of the probationary process shall be discussed and agreed between the employee and the direct line manager/supervisor. The outcome of the probationary period is expected to be a confirmation of the job role, some amendment to the role and/or provision of additional staff development.

The onboarding / probationary period leads into and may occur in concert with employee training and awareness - employee training/staff development plan.

Employment lifecycle - not applicable to suppliers

Employment lifecycle

Employment of individuals shall be subject to annual performance review throughout the employment lifecycle and also when changes occur in the employees role within the organisation.

Employment lifecycle individual training/staff development plans and records including ISMS needs are developed and retained.

Disciplinary process

Management of the disciplinary process is the domain of the Human Resources Officer with advice from an IT Representative for IT related activities.

All Information related to disciplinary processes shall be treated confidentially and held only on the employee restricted file. Management personnel involved in any disciplinary process shall be subject to the company confidentiality standards.

This process must be approved by an executive role and shall only be managed by the HR Officer and relevant IT Representative in consultation with the direct line manager pertinent to the intended disciplinary activity.

The HR Manager shall ensure the documented process includes:

- nature and consequences of the IT breach
- circumstances of the breach - malicious or unintentional
- previous history related to the issue

Human Resources Policy

- impact of training and staff development as a contributor

Jurisdictional legal and regulatory requirements and employment contractual agreements shall be met in all disciplinary matters.

Termination or change of employment or contract (includes suppliers)

Information security aspects of an individual's employment or contracted duties including IS access controls must be considered in the case of employment change or contract termination.

On termination of a contract or duties of an employee changes, the information security access afforded the individual and their duties shall be considered and an arrangement made regarding its end point - at actual termination or a post termination point where a contract may partially continue or phase out. The validity of such arrangements is subject to ICT executive approval for high risk roles.

Where transition or transfer of IS responsibilities to a new or existing role within the organisation occurs, this shall be documented and approved by an ICT executive role prior to implementation.

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. Refer below for the most recent review.

History table

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