1. **Scope**[[1]](#footnote-1)

All individuals who will be allowed to access organisational information assets are subject to pre-employment screening and subsequent terms and conditions of employment, as well as other conditions on behavior and discipline while performing work under *{OrganisationName}*’s control.

1. **Responsibilities**
   1. The *{HRDept}* is responsible for carrying out screening checks on all candidates for employment, contractors and third party users of organisational information systems prior to their employment being finalised.
   2. The *{HRDept}* is also responsible for ensuring that employees and contractors are aware of and fulfil their information security responsibilities.
   3. The *{HeadHR},* individual *{Manager}* have specific responsibilities as detailed below.
   4. All Employees/Staff and contractors are responsible for ensuring they abide by the requirements of their employment.
2. **Screening**
   1. All individuals allowed to access *{OrganisationName}* information assets must satisfy both the *{HeadHR}* and the immediate *{Manager}* in respect of:
   2. Satisfactory *[written]* character references
   3. Accuracy of curriculum vitae (i.e. previous employers confirm dates, positions, etc.)
   4. Confirmation of claimed qualifications (professional and academic)
   5. Identity (passport check)
   6. All individuals who will have access to restricted or confidential information must also receive satisfactory [ ] checks.
   7. In situations where an individual does not satisfactorily meet these requirements, the *{HeadHR}* and the immediate *{Manager}* must agree whether the appointment can proceed (given the business requirements, the classification of the data and the risk assessment) and any decision they make will be documented in the applicant’s file. In case of disagreement, the appointment is referred to the *{ChiefInfoSecOfficer})* or the *{ChiefExecutiveOfficer}*, as appropriate, whose decision will be final.
   8. Screening information about candidates is classified as confidential.

1. **Terms and conditions of employment**
   1. Employees and contractors agree and sign the terms and conditions of their employment contract, which state their and *{OrganisationName}*’s responsibilities for information security.
2. **Management responsibilities**
   1. Management requires employees and contractors to apply security in accordance with the policies and procedures of *{OrganisationName}*’s ISMS.
   2. Management ensures that employees, contractors and third parties are appropriately briefed prior to being granted access to *{OrganisationName}* information assets.
   3. Management ensures that employees, contractors and third parties receive guidelines on security expectations (User Agreement, job descriptions and terms and conditions of employment).
   4. Management provides personal leadership and example in information security and ensures that *{OrganisationName}*’s policies and procedures are followed.
3. **Information security awareness, education and training**
   1. All employees of *{OrganisationName}* and, where relevant, contractors receive appropriate awareness training and regular updates in *{OrganisationName}* policies and procedures, as relevant for their job function.
   2. The *{HeadHR}* is responsible for ensuring that all users receive standard information security induction and awareness training before they are allowed to access *{OrganisationName}* information assets. This is conducted on the basis of a training needs analysis, and includes the incident reporting procedure.
   3. The Information Security Manager is responsible for ensuring that all users receive regular updates and alerts on information security issues as and when necessary, and that additional security-related training is made available as and when required.
   4. The Information Security Manager is responsible for ensuring that specialised information security staff receive appropriate specialist training in line with their job requirements.
4. **Disciplinary process**
   1. *{OrganisationName}* has a formal disciplinary process that applies to employees who have committed an information security breach.
   2. This process operates in accordance with *{OrganisationName}*’s Disciplinary Policy ([document reference and link]).

1. **Termination and change of employment**
   1. Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated to the employee or contractor, and enforced.
   2. Upon termination or change of employment, a termination checklist ([ISMS-C REC 7.3.1](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_7.3.1.docm)) is completed and returned to HR.

***Document Owner and Approval***

The *{HeadHR}* is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to *[all/specified]* members of staff on the *[corporate intranet]* and is published *[ ].*

This procedure was approved by the *{Manager}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |

1. **Chapter 9** [*IT Governance: An International Guide to Data Security and ISO27001 / ISO27002*](http://www.itgovernance.co.uk/shop/p-772-it-governance-an-international-guide-to-data-security-and-iso27001iso27002.aspx)provides guidance on the HR controls. This procedure will need to be drafted (taking into account the clauses here already) by the *[{HeadHR}]* (or an appropriate delegate) and will need to take into account your existing procedures for screening potential *[employees/staff].* In other words, this procedure is an extension to what you do now, both in terms of the depth of the screening (and tying it to specific information security issues) and in terms of the range of people who should be screened. [↑](#footnote-ref-1)