1. **Scope**

All supplier relationships with *{OrganisationName}* involving information assets are within the scope of this policy.

This includes suppliers involved in the storage, transmission and processing of information, even where the information is encrypted or otherwise generally inaccessible to the supplier.

1. **Responsibilities**
2. The *{InfoSecManager}* is responsible for ensuring that all relationships take information security into account at the first instance.
3. All relationship *[owners]* responsible for services in any of the above categories are required to ensure that external parties have entered into a formal external party agreement.
4. Relationship *[owners]* are responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.
5. The *{InfoSecManager}* is responsible for carrying out risk assessments (see [ISMS DOC 6](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Section_4-10/ISMS_DOC_6.docm)) where required by this procedure.
6. **Information security policy for supplier relationships**
   1. *{OrganisationName}* treats information security within supplier relationships as an extension of the ISMS.
   2. All supplier relationships are subject to a risk assessment prior to any exchange or delivery of information assets.
   3. *{OrganisationName}* takes the following into account when considering and conducting supplier agreements:
      1. The business case for supply chain security
      2. Information risk within the supply chain, and associated threats
      3. The nature of the relationship – acquisition or supply of information assets
      4. Organisational capability of assuring information security, with regard to both *{OrganisationName}* and the supplier
      5. System lifecycle processes for the assurance of information security
      6. ISMS processes and controls in relation to system lifecycle processes
      7. ISMS processes and controls in relation to security of the supply chain
      8. Essential security practices within the supply chain
7. **Addressing security in third party agreements**
8. *{OrganisationName}* carries out a risk assessment (in line with the requirements of procedure ISMS DOC 6) to identify risks related to external party access.
9. Controls are selected in line with the requirements of ISMS DOC 6.
10. *{OrganisationName}* implements those controls that are within its own power.
11. *{OrganisationName}* agrees with the external party those controls that the external party is required to implement and documents them in an agreement (drawn up by *{OrganisationName}*’s legal advisers) that the third party signs.
12. The agreements between *{OrganisationName}* and external parties are created by *{OrganisationName}*’s legal advisers.
13. **Information and communication technology supply chain**
    1. Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.
14. **Monitoring and review of supplier services**
    1. The external party agreement includes reporting structures, defines acceptable levels of performance and provides monitoring, inspection and audit rights.
    2. The relationship *[owner]* monitors performance against the service and security criteria contained in the agreement by *[insert detail of how this is done in general]*, ensures that reports required under the agreement are delivered as required and reviews them, and conducts regular progress meetings as required.
    3. The relationship *[owner]* ensures that information security incidents experienced by the third party are reviewed jointly and that relevant information security incidents experienced internally are communicated to the third party to that appropriate steps can be taken.
    4. The relationship *[owner]* identifies any problems of any sort on either side of the relationship, and ensures that they are resolved, using the agreed escalation procedure where necessary.
    5. The *{QualityManager}* is responsible for reviewing the third party’s internal audit trails and records of security events.
    6. On a *[monthly]* basis, the *{HeadIT}* reviews all outstanding actions in respect of deficiencies in third-party services to ensure that appropriate corrective or preventative action is being taken, having regard to the fact that ultimate responsibility for the information processed by the third party remains with *{OrganisationName}*.
15. **Managing changes to supplier services**

*{OrganisationName}* may need to agree changes to external party contracts and agreements to take account of changes that it makes to, or as a result of:

1. the services it currently offers to its clients;
2. new applications and systems it has developed or acquired;
3. modifications, changes or updates to its own policies and procedures;
4. new or amended controls arising from new risk assessments or information security incidents.
   1. The external party may need to request changes to the contract in order to implement:
5. Changes or improvements to their networks or other infrastructure.
6. New or improved technologies, new products or new releases of current products.
7. New development tools, methodologies and environments.
8. New physical locations or physical services.
9. New vendors or other suppliers of hardware, software or services.
   1. Any changes that may be required are subject to a new risk assessment (taking into account the criticality of the business systems involved) and review of the selected controls.
   2. New controls, or changes to existing controls are identified, authorised, agreed with the third party, and made the subject of an agreed variation [insert here a reference to exactly how contract variations are handled] to the existing contract.
   3. The relationship *[owner]* is responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.

***Document Owner and Approval***

The *{InfoSecManager}* 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 *{ChiefInfoSecOfficer}* 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 |
|  |  |  |  |
|  |  |  |  |