Contract and Supplier Security
Example Policy

Author: R Rutherford
Date: 24/05/2017
Version: 1.0
## Contents

1. Purpose 3
2. Scope 3
3. Applicability 3
4. Guidance 3

**Terminology** 3

**Policy** 3

| General 3 |
| Assesing Outsourcing Risks 4 |
| Contracts and Confidentiality Agreements 4 |
| Hiring and Training of Staff (Employees and Third Party) 6 |
| Access controls 7 |
| Security audits 8 |
| Responsibilities 8 |

5. Key Words 9
1 Purpose

The purpose of this Contract and Supplier Security Example Policy is to provide exemplar guidance in line with HMG and private sector best practice for the implementation of an organisation wide Contract and Supplier Security Policy. This is in order to allow the reader to produce the necessary policies and guidance for their business area in line with the Department for Health, the wider NHS, health and social care and HMG requirements.

2 Scope

The drafting of any policy governing Contract and Supplier Security is in support of NHS or health and social care business functions.

3 Applicability

This Example Policy is applicable to and designed for use by any NHS, health and social care or associated organisations that use or have access to NHS systems and/or information and data at any level.

4 Guidance

This Example Policy provides guidance on the production of a Contract and Supplier Security Policy. The Example Policy is in italics with areas for insertion shown as <> and the rationale for each paragraph or section, where required, in […].

Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning/Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHALL</td>
<td><em>This term is used to state a Mandatory requirement of this policy</em></td>
</tr>
<tr>
<td>SHOULD</td>
<td><em>This term is used to state a Recommended requirement of this policy</em></td>
</tr>
<tr>
<td>MAY</td>
<td><em>This term is used to state an Optional requirement</em></td>
</tr>
</tbody>
</table>

Policy

General

- <Insert organisation name> **shall** ensure that a full assessment of the potential security risks with using an outsourced provider or a supplier is carried out.

- <Insert organisation name> **shall** ensure that the risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, technical, procedural and managerial controls.

- <Insert organisation name> **should** consider the following when selecting an outsourced provider or a supplier:
• Supplier’s reputation and history.
• Quality of services provided to other customers.
• Financial stability of the company and commercial record.
• Retention rates of the company’s employees.
• Quality assurance and security management standards currently followed by the company (e.g. certified compliance with ISO 9001 and ISO/IEC 27001).

[Organisations must ensure that any potential contractors and/or suppliers at all levels are carefully researched before they are chosen and that any risks associated with the use of contractors or suppliers are identified, assessed and managed. Failure to do so could have severe consequences for the organisation, should any unidentified or unmanaged risks be realised.]

### Assessing Outsourcing Risks

- **<Insert organisation name> shall** ensure that a suitable owner is nominated for each business function/process outsourced.
- **<Insert organisation name> shall** ensure that in relation to outsourcing, specifically, the risk assessment shall take due account of the:
  - Nature of logical and physical access to <insert organisation name> information assets and facilities required by the outsourced provider or a supplier to fulfil the contract;
  - Sensitivity, security classification, volume and value of any information assets involved.
  - Commercial risks such as the possibility of the outsourced provider’s or supplier’s business failing completely or of them failing to meet agreed service levels.
  - Security and commercial controls known to be currently employed by the outsourced provider or the supplier.
  - The result of the risk assessment shall be presented to <insert organisation name> management for approval prior to signing the outsourcing contract.

[The outsourcing of any service or process will bring risks additional to those realised by just running the service or process. These additional risks to the service or process should be identified and thoroughly assessed and a risk balance decision should be made before the organisation considers outsourcing any service or process.]

### Contracts and Confidentiality Agreements

- A formal contract between <insert organisation name> and the outsourced provider or the supplier shall exist to protect both parties.
- The contract shall clearly define the types of information exchanged and the purpose for so doing.
- If the information being exchanged holds a security classification or is sensitive, a binding confidentiality agreement shall be in place between <insert organisation
name> and the outsourced provider or the supplier, whether as part of the outsourced contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).

- Information **shall** be security classified and controlled in accordance with NHS and HMG policy and best practice.
- Any information received by <insert organisation name> from the outsourced provider or the supplier which is bound by the contract or confidentiality agreement **shall** be protected by appropriate security classification and labelling.
- Upon termination of the contract, the confidentiality arrangements **shall** be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.
- All contracts **shall** be submitted to the Legal department for accurate content, language and presentation.
- All contracts **shall** clearly define each party’s security responsibilities toward the other by defining:
  - The parties to the contract.
  - Effective date.
  - Functions or services being provided.
  - Liabilities.
  - Limitations on use of sub-contractors.
  - Any other security matters normal to any contract.
  - Legal, regulatory and other third party obligations such as data protection/privacy laws, money laundering etc.
- Depending on the results of the risk assessment, information security obligations and controls **shall** be embedded or referenced within the contract, such as:
  - Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System (ISMS) such as that defined in ISO/IEC 27001.
  - Background checks on employees or third parties working on the contract.
  - Access controls to restrict unauthorised disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities etc.
  - Information security incident management procedures including mandatory incident reporting.
  - Return or destruction of all information assets by the outsourced provider or the supplier after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity.
- Copyright, patents and similar protection for any intellectual property shared with the outsourced provider or the supplier, or those developed in the course of the contract.

- Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow.

- Anti-virus, anti-malware, anti-spam and similar controls.

- IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks.

- The right of <insert organisation name> to monitor all access to and use of <insert organisation name> facilities, networks, systems etc., and to audit the outsourced provider’s or the supplier’s compliance with the contract, or to employ a mutually agreed independent third party auditor for this purpose.

- Business continuity arrangements including crisis and incident management, resilience, backups and IT Disaster Recovery.

- Although outsourced providers and suppliers that are certified compliant with ISO/IEC 27001 can be presumed to have an effective ISMS in place, it may still be necessary for <insert organisation name> to verify security controls that are essential to address specific security requirements.

[Once a decision is made to outsource a service or process, or employ the services of a supplier, organisations must ensure that the relevant and required security controls are documented within any contract and confidentiality agreement. These should be in line with the organisation’s own internal security policies. The contract should also include details of how these will be verified (i.e. through supplier compliance visits, inspections or documentary evidence). The section above should detail the minimum requirements.]

**Hiring and Training of Staff (Employees and Third Party)**

- Outsourced employees, contractors and consultants working on behalf of <insert organisation name> shall be subjected to background checks equivalent to those performed on <insert organisation name> employees. Such screening should cover:
  - Proof of the person’s identity (e.g. passport).
  - Proof of UK National Security Vetting Standard (at required level).
  - Proof of their academic qualifications (e.g. certificates).
  - Proof of their work experience (e.g. résumé/CV and references).
  - Criminal record check
  - Credit check.

- Suppliers providing contractors/consultants directly to <insert organisation name> or to outsourced providers used by <insert organisation name> shall perform at least the same standard of background checks as those indicated above.
Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to <insert organisation name> information security policies, standards, procedures and guidelines (e.g. privacy policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract.

[Organisations should ensure that the relevant background checks (to the required and relevant standard) are carried out on any potential employees or contractors before they are given any access to security classified or sensitive systems, services or information. The level of these checks will be dependent on the level and type of access the potential employees or contractors are given, but organisations must take into account that this level may increase considerably once the potential employee or contractor is taken in to the organisation. All employees and contractors should also be provided with the necessary education, awareness and training in order for them to carry out their role and protect the organisation’s systems, services and information to the required standard. This includes providing the employee or contractor with access to all relevant policies, standards, guidelines and procedures.]

Access controls

In order to prevent unauthorised access to <insert organisation name> information assets by the outsourced provider, supplier or sub-contractors, suitable security controls shall be implemented.

Technical access controls shall include:

- User identification and authentication.
- Authorisation of access, through the assignment of users to defined user roles having appropriate logical access rights and controls.
- Data encryption in accordance with <insert organisation name> encryption policies and standards.
- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

Procedural access controls shall include:

- Strong passwords.
- Determining and configuring appropriate logical access rights.
- Reviewing and if necessary revising access controls to maintain compliance with requirements.

Physical access controls shall include:

- Layered controls covering perimeter and internal barriers.
- Strongly-constructed facilities.
- Suitable locks with key management procedures.
• Access logging through the use of automated key cards, visitor registers etc.
• Intruder alarms/alerts and response procedures.
• If parts of <insert organisation name> IT infrastructure are to be hosted at a third party data centre, assets are both physically and logically isolated from other systems.
• <Insert organisation name> shall ensure that all information assets handed over to the outsourced provider during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract.

[Organisations should ensure that access to systems, services and information is provided on a ‘Need to Know’ basis and in line with the organisation’s security policies, (Access Control, Data Handling, etc).]

Security audits

• If <insert organisation name> outsources a business function to a different location, it shall audit the outsourced provider’s physical premises periodically for compliance to <insert organisation name> security policies, ensuring that it meets the requirements defined in the contract.
• Any audit shall also take into consideration the service levels agreed in the contract, determining whether they have been met consistently and reviewing the controls necessary to correct any discrepancies.
• The requirement for any audit shall be defined in the contract.
• The frequency of any audit shall be determined by <insert organisation name> management.

[Organisations should ensure that they include within any outsource or supplier contracts the requirement to audit and verify security arrangements, processes and procedures at the suppliers premises and any other relevant locations.]

Responsibilities

• <Insert organisation name> Management:
  • Management shall be responsible for designating suitable owners of business processes that are outsourced, overseeing the outsourcing activities and ensuring that this policy is followed.
  • Management shall be responsible for mandating commercial or security controls to manage the risks arising from outsourcing.
• <Insert organisation name> Information Security Team:
  • <Insert organisation name> Information Security Team, in conjunction with functions such as Legal, Compliance and Risk Management, shall be responsible for assisting outsourced business process owners to analyse the associated risks and develop appropriate process, technical, physical and legal controls.
• <Insert organisation name> Information Security Team shall be responsible for maintaining this policy.

[This section should cover the responsibilities within the organisation for the management of contractor and supplier security. Organisations should consider areas such as but not limited to: general security management, security risk management, security incident management, security education and awareness, security audit and compliance and any related legal and legislative issues. The examples provided above represent the minimum requirement and these should be tailored dependant on the size and structure of the organisation and the type of services and processes outsourced by the organisation.]

5 Key Words