NHS Digital

Contract and Supplier Security

Upstream Outcomes Policy

(Supporting Bridgit Care & Upstream Health Business Units)

Author: D Crombie

Date: 04/04/2022

Version: 2.0

Information and technology
for better health and care

Contents

1 Background

This policy is based on NHS Digitals example policy and aligns to the recommendations and approach adopted by NHS Digital. This is based on the NHS Digital template dated 23rd May 2017.

2 Approval / update history

Version ID	Description	SIRO Approval
1.0	Initial version for release	08/10/2018 : Darren Crombie
2.0	Updated version following 2022 review	05/04/2022 : Darren Crombie

Terminology

Term	*Meaning/Application*
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

Policy

General

- *Upstream Outcomes **shall** ensure that a full assessment of the potential security risks with using an outsourced provider or a supplier is carried out.*
- *Upstream Outcomes **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.*
- *Upstream Outcomes **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).*

Assessing Outsourcing Risks

- *Upstream Outcomes **shall** ensure that a suitable owner is nominated for each business function/process outsourced.*
- *Upstream Outcomes **shall** ensure that in relation to outsourcing, specifically, the risk assessment shall take due account of the:*
    - *Nature of logical and physical access to Upstream Outcomes 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 Upstream Outcomes management for approval prior to signing the outsourcing contract.*

Contracts and Confidentiality Agreements

- *A formal contract between Upstream Outcomes 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 Upstream Outcomes 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 Upstream Outcomes 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 Upstream Outcomes to monitor all access to and use of Upstream Outcomes 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 Upstream Outcomes to verify security controls that are essential to address specific security requirements.*

Hiring and Training of Staff (Employees and Third Party)

- *Outsourced employees, contractors and consultants working on behalf of Upstream Outcomes* ***shall*** *be subjected to background checks equivalent to those performed on Upstream Outcomes 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 Upstream Outcomes or to outsourced providers used by Upstream Outcomes* ***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 Upstream Outcomes 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.*

Access controls

- *In order to prevent unauthorised access to Upstream Outcomes 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 Upstream Outcomes 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 though the use of automated key cards, visitor registers etc.*
  - *Intruder alarms/alerts and response procedures.*
  - *If parts of Upstream Outcomes IT infrastructure are to be hosted at a third party data centre, assets are both physically and logically isolated from other systems.*

- *Upstream Outcomes **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.*

Security audits

- *If Upstream Outcomes outsources a business function to a different location, it **shall** audit the outsourced provider's physical premises periodically for compliance to Upstream Outcomes 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 Upstream Outcomes management.*

Responsibilities

- *Upstream Outcomes 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.*
- *Upstream Outcomes Information Security Team:*
  - *Upstream Outcomes 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.*
  - *Upstream Outcomes Information Security Team **shall** be responsible for maintaining this policy.*

3 Key Words

Access, Audit, Business Continuity, Confidentiality, Configuration, Controls, Copyright, Contract, Destruction, Disaster Recovery, Disclosure, Information, Intellectual Property, ISMS, IT Systems, Legal, Malware, Non-disclosure, Outsource, Patching, Patents, Risk, Security Classification, Sensitivity, Service Levels, Supplier, Vetting, Virus