Supplier Security Policy

Policy Number	48
Version	2
Policy Contact	Matthew Betteridge
Date Issued	05th March 2024
Review Date	06th May 2026
Next Review Date	06th May 2027
Approved by	OneCall24 Policy Team

Introduction

Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally) to an outsourcer for an agreed charge. The outsourcer provides services to the customer based on a mutually agreed service level, normally defined in a formal contract.

Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:

- Reducing the organisation's costs
- Greater focus on core business by outsourcing non-core functions.
- Access to world-class skills and resources

Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection or the inability of the outsourcer to live up to agreed service levels, would reduce the benefits, and could jeopardise the security posture of the organisation.

This policy aligns with the requirements of the Data Security and Protection Toolkit, applicable UK legislation including the UK GDPR and the Data Protection Act 2018, and supports the organisation's quality management system under ISO 9001.

Objective

This policy specifies controls to reduce the information security risks associated with outsourcing.

Scope

The policy applies throughout One Call 24 Limited (OneCall24).

Outsourcing providers (also known as outsourcers) include:

- hardware and software support and maintenance staff
- external consultants and contractors
- IT or business process outsourcing firms
- temporary staff

Policy axioms

The commercial benefits of outsourcing non-core business functions must be balanced against the commercial and information security risks.

The risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural, and managerial controls.

Choosing an outsourcer

Criteria for selecting an outsourcer shall be defined and documented, considering the:

- company's reputation and history.
- quality of services provided to other customers.
- number and competence of staff and managers.
- financial stability of the company and commercial record.
- retention rates of the company's employees.
- alignment with OneCall24's quality management standards (e.g., processes consistent with ISO 9001)
- Evidence of information security controls appropriate to the level of risk (e.g., policies, certifications, or independent assurance)

Further information security criteria may be defined as the result of the risk assessment (see next section).

Assessing outsourcing risks

Management shall nominate a suitable OneCall24 owner for each business function/process outsourced. The owner, with help from the Management Team, shall assess the risks before the function/process is outsourced, using IFB standard risk assessment processes.

In relation to outsourcing, specifically, the risk assessment shall take due account of the:

- nature of logical and physical access to IFB information assets and facilities required by the outsourcer to fulfil the contract.
- sensitivity, volume, and value of any information assets involved.
- commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to OneCall24 competitors where this might create conflicts of interest; and
- security and commercial controls known to be currently employed by OneCall24 and/or by the outsourcer.
- Impact on service quality and delivery in line with ISO 9001 requirements

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if OneCall24 will benefit overall by outsourcing the function to the outsourcer, considering both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g., if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

Suppliers may be categorised based on risk (e.g. high, medium, low) depending on the nature of the services, access to systems, and sensitivity of data. The level of due diligence, monitoring, and audit will be proportionate to this risk classification.

All outsourcing arrangements must be formally approved by management prior to contract signature.

Contracts and confidentiality agreements

All suppliers must have a formally executed contract in place prior to the commencement of services.

Where personal or sensitive information is involved, a non-disclosure agreement (NDA) and/or confidentiality clause is mandatory.

Any exceptions must be formally risk assessed, documented, and approved by senior management and Information Security prior to engagement.

Where suppliers process personal data on behalf of OneCall24, a Data Processing Agreement (DPA) must be in place in accordance with the UK GDPR.

If the information being exchanged is sensitive, a non-disclosure agreement shall be in place between OneCall24 and the outsourcer (Where applicable), Information shall be classified and controlled in accordance with OneCall24 Classification requirements.

Any information received by OneCall24 24 from the outsourcer which is bound by the contract or non-disclosure agreement shall be protected by appropriate classification and labelling.

Upon termination of the contract or non-disclosure agreement the company shall determine whether to extend the tenure of the contract/non-disclosure agreement.

Hiring and training of employees

Outsource employees, contractors and consultants working on behalf of OneCall24 shall be subjected to background checks equivalent to those performed on OneCall24 employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):

- Proof of the person's identity (e.g., passport).
- Proof of their academic qualifications (e.g., certificates).
- Proof of their work experience (e.g., résumé/CV and references).
- Criminal record check.
- Credit check.

Companies providing contractors/consultants directly to OneCall24 or to outsourcers used by OneCall24 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 OneCall24 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 OneCall24 information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design a suitable controls architecture.

Technical access controls shall include:

- User identification and authentication.
- Authorisation of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls.
- Data encryption in accordance with OneCall24 encryption policies and standards defining algorithms, key lengths, key management, etc.

- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

Procedural components of access controls shall be documented within procedures, guidelines and related documents and incorporated into awareness, training, and educational activities. This includes:

- Choice of 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 OneCall24 24's IT infrastructure are to be hosted at a third-party data centre, the data centre operator shall ensure that OneCall24 24 assets are both physically and logically isolated from other systems.

OneCall24 24 shall ensure that all information assets handed over to the outsourcer during 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. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

Security audits

If OneCall24 24 has outsourced a business function to an outsourcer based at a different location, it shall audit the outsourcer's physical premises periodically for compliance to OneCall24 24 security policies, ensuring that it meets the requirements defined in the contract.

The 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 frequency of audit shall be determined by management on advice from functions such as Internal Audit, Information Security Management and Legal.

Supplier performance and compliance shall also be reviewed in line with OneCall24's quality management processes under ISO 9001.

Responsibilities

Management

Management is responsible for designating suitable owners of business processes that are outsourced, overseeing the outsourcing activities, and ensuring that this policy is followed.

Management is responsible for mandating commercial or security controls to manage the risks arising from outsourcing.

Management is responsible for ensuring supplier management activities align with the organisation's quality management system under ISO 9001

Outsourced business process owners

Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

Information Security

Compliance, in conjunction with functions such as Legal and Risk Management, is responsible for assisting outsourced business process owners to analyse the associated risks and develop appropriate process, technical, physical, and legal controls.

Compliance is also responsible for maintaining this policy.

Internal Audit

Internal Audit is authorised by management to assess compliance with all corporate policies at any time.

Internal Audit may assist with audits of outsourcing contracts including security compliance audits and advise management on the risks and controls relating to outsourcing.

Suppliers must notify OneCall24 of any actual or suspected information security incident or personal data breach immediately and no later than 24 hours after discovery.

OneCall24 shall assess whether notification to the Information Commissioner's Office or NHS authorities is required within statutory timeframes.

Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.