

## Supplier Security Policy

Policy Number	91
Version	1
Policy Contact	Matthew Betteridge
Date Issued	05 <sup>th</sup> March 2024
Review Date	06 <sup>th</sup> May 2025
Next Review Date	06 <sup>th</sup> May 2026
Approved by	OneCall24 Policy Team

## Contents

<b>1. Introduction.....</b>	<b>3</b>
<b>2. Objective .....</b>	<b>3</b>
<b>3. Scope.....</b>	<b>3</b>
<b>4. Policy axioms.....</b>	<b>3</b>
<b>5. Choosing an outsourcer .....</b>	<b>3</b>
<b>6. Assessing outsourcing risks .....</b>	<b>4</b>
<b>7. Contracts and confidentiality agreements .....</b>	<b>4</b>
<b>8. Hiring and training of employees .....</b>	<b>5</b>
8.1. Access controls .....	5
8.2. Security audits .....	6
<b>9. Responsibilities.....</b>	<b>6</b>
9.1. Management .....	6
9.2. Outsourced business process owners.....	6

## 1. 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.

## 2. Objective

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

## 3. 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

## 4. 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.

## 5. 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.
- ❖ quality assurance and security management standards currently followed by OneCall24(e.g., certified compliance with ISO 9001).

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

## 6. 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.

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.

## 7. Contracts and confidentiality agreements

The management team of OneCall24 reserve the right to approve/choose suppliers when no non-disclosure agreement or contract or service provider agreement is in place dependable on the level of risk. See risk methodology in risk assessment risk treatment plan register.

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.

## 8. 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.

### 8.1. 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 through 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 datacentre 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.

## 8.2. 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.

## 9. Responsibilities

### 9.1. 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.

### 9.2. 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.

#### 9.2.1. 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.

#### 9.2.2. 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.