



A Uniti  
Group  
Company

A decorative graphic on the left side of the page consisting of a cluster of green circles of various sizes, arranged in a pattern that tapers from left to right.

# Supplier Standards and Guidelines



**OPTICOMM**  
Networks

## Disclaimer

The information in this document is provided for general information purposes only. Recipients must make their own inquiries as to the accuracy and completeness of information contained in this document. Opticomm may update this document from time to time.

© Opticomm Pty Ltd 2024. All rights reserved.

Please consider the environment before printing this document.

## Change History

Version	Description	Effective Date
1.0	New Policy	3 June 2024

## Changes in this revision

The detailed changes to this document, from Version 1.0 dated 3 June 2024 to Version 1.1 are outlined in the table below.

Version	Description
1.1	

## Contents

1	Introduction .....	4
1.1	Purpose.....	4
1.2	Scope.....	4
1.3	Definitions and Interpretations.....	4
2	Professional Conduct.....	5
2.1	General principles .....	5
2.2	Confidential information .....	5
2.3	Conflicts of interest.....	6
2.4	Bribery and corruption.....	6
3	Induction .....	6
3.1	Screening and Police Checks .....	6
3.2	Work Health and Safety .....	7
4	Environmental Management .....	7
4.1	Environmental Impact .....	<b>Error! Bookmark not defined.</b>
5	Modern Slavery and Labour Practices .....	8
5.1	General Principles.....	8
5.2	Modern Slavery .....	8
6	Cyber Security and Privacy.....	9
6.1	Security Policies.....	9
6.2	Supplier Devices .....	9
7	Notifiable incidents .....	9
7.1	WHS/OH&S Incidents .....	9
7.2	Other Incidents.....	10

# 1 Introduction

## 1.1 Purpose

This document sets out minimum standards and guidelines by which all suppliers to Opticomm, including contractors, consultants and their business and supply chains, must adhere to when working with, and for Opticomm. This is a requirement regardless of whether or not this document has been formally incorporated into a contract between Opticomm and the supplier.

## 1.2 Scope

This document describes the requirements and responsibilities of all suppliers including:

- health and safety;
- cyber security and privacy;
- labour, human rights and modern slavery; and
- anti-bribery and corruption.

## 1.3 Definitions and Interpretations

Definitions used in this document are outlined in the table below or otherwise in accordance with the standard usage in the telecommunications industry.

Table 1 - Definitions

	Definition
Alleged Misconduct	means an allegation which raises a reasonable suspicion of misconduct which may have a serious impediment to the delivery of the Services or the performance of activities under or in relation to the Services, including serious or persistent harassment or bullying, or a criminal offence such as theft, fraud or assault.
Incident Reporting Portal	means the portal located at <a href="#">Opticomm Incident reporting Portal</a>
Modern Slavery	describes situations where coercion, threats or deception are used to exploit victims and undermine or deprive them of their freedom. It describes serious exploitation and does not include practices like substandard working conditions or underpayment of workers.
Notifiable Incident	means any incident listed in clause 7

Serious Incident	means an incident that: <ul style="list-style-type: none"> <li>(a) is likely to impact on the Supplier's ability to deliver the Services;</li> <li>(b) arises in respect of work, health and safety in connection with the delivery of the Services;</li> <li>(c) involves Modern Slavery;</li> <li>(d) requires an emergency response, or involves death or serious injury or any criminal activity; and</li> <li>(e) arises in respect of incident notification under WHS/OH&amp;S law concerning <b>notifiable or dangerous incidents</b>.</li> </ul>
Services	means the services supplied to Opticomm by the Supplier either directly or through its contractors or subcontractors
Supplier	includes any suppliers, contactors and their subcontractors.
SWMS	means safe working method statements

## 2 Professional Conduct

### 2.1 General principles

Opticomm expects high standards of professional conduct and compliance with all applicable laws from its suppliers.

Suppliers and their personnel are expected to:

- maintain appropriate standards of behaviour, conduct and ethics in their dealings with Opticomm, its customers and other suppliers;
- comply with all applicable anti-bribery, anti-corruption and anti-money laundering laws;
- not engage in, either directly or indirectly, fraudulent, corrupt or collusive activities;
- conduct themselves in a manner that is fair, professional and will not bring Opticomm into disrepute; and
- be ethical in their business activities, including relationships, practices, and operations.

### 2.2 Confidential information

Suppliers must not improperly use any private, confidential or commercially sensitive information in its possession relating to or in connection with its dealings with Opticomm and will have appropriate cyber security policies and processes in place to protect Opticomm's confidential information. Suppliers will not publicly comment about their relationship with Opticomm without prior consent.

## 2.3 Conflicts of interest

Suppliers must declare to Opticomm any situation that raises an actual, potential or perceived conflict of interest related to or in connection with its dealings with Uniti and avoid financial, business or other relationships which may compromise the performance of their duties under their business arrangement with Opticomm.

## 2.4 Bribery and corruption

Suppliers should not attempt to bias a decision or gain business or commercial benefit for themselves or Opticomm by promising, giving, requesting or agreeing to receive or accept bribes or payments of any kind.

Whilst Opticomm supports reasonable and proportionate giving and receiving of hospitality as part of a normal business relationship, we prohibit the giving and receiving of any gifts or hospitality that are excessive or improper.

# 3 Induction

All Suppliers are required to upload information via the Opticomm supplier portal, currently CM3.

## 3.1 Screening and Police Checks

- (a) Suppliers must conduct a thorough interview and evaluation process for all supplier personnel proposed to be engaged to carry out the Services including:
  - (i) confirmation of identity with photo identification being either a passport or driver's licence;
  - (ii) obtaining a clear police check through the Australian Federal Police at the supplier's cost;
  - (iii) checking professional and personnel references.
- (b) The screening process must include a signed declaration from each prospective Supplier personnel that:
  - (i) they consent to a police check;
  - (ii) they have no current or prior criminal charges or convictions or if they do have such charges or convictions, they must state the nature of the charge, offence, or conviction in the declaration; and
  - (iii) they acknowledge that the supplier will obtain references from two previous employers.
- (c) Where applicable, the Supplier shall ensure that all staff and/or sub-contractors have passed a recent (no more than 12 months) screening check complying with relevant legislation in relation to working around children before attending a site where children are present (i.e. schools/day care centres etc.).

- (d) The Supplier will provide a compliance report to Opticomm in respect of all screening, checks and declarations monthly or upon request at any time.

### 3.2 Work Health and Safety

Where the Services or any part of the Services are required to be performed on Opticomm's premises or any premises of any other third party, the Supplier will ensure that:

- (a) all of its employees and sub-contractors and their employees have completed Opticomm's induction programme and training as is necessary to enable the employees and sub-contractors to perform their work in a manner that is safe and without risks to health in accordance with all work health and safety legislation as is applicable to the supplier (WHS/OH&S Legislation);
- (b) it will perform site readiness assessments in accordance with the direction of Opticomm, including via any Opticomm portal or application;
- (c) SWMS will be subject to checklisting before use. Any shortcomings must be rectified by the supplier or will be directed to work under Opticomm SWMS;
- (d) will comply with a direction from Opticomm requiring the removal of any persons who, in the reasonable opinion of Opticomm, are guilty of misconduct, incompetence or negligence in the performance of their duties; and
- (e) will comply with, have in place adequate and appropriate safety management systems & safe systems of work for compliance with, and ensure that any and all subcontractors or other persons engaged in the performance of the Services, comply with the requirements of all applicable WHS/OH&S Legislation and all codes of practice and standards relevant to the performance of the Services.

## 4 Environmental Management

- (a) Suppliers must comply with all relevant statutory and regulatory requirements.
- (b) Suppliers should assess the environmental impact of their activities and wherever possible, mitigate its impact in planning, building operating and decommissioning activities.
- (c) Packaging and associated materials must be reduced, recycled or reused wherever possible.
- (d) Any environmental incidents must be reported via the [Opticomm Incident reporting Portal](#).

# 5 Modern Slavery and Labour Practices

## 5.1 General Principles

- (a) Suppliers are expected to provide a fair, safe and healthy workplace, free of Modern Slavery, which upholds high standards of human rights and integrates appropriate safety, human rights and labour policies and practices into their business.
- (b) Suppliers are expected to:
  - (i) maintain a workplace which is free from bullying, harassment, discrimination and victimisation;
  - (ii) observe all laws and regulations with respect to wages, working hours, overtime, maximum hours and workers compensation insurance;
  - (iii) pay all workers their legally mandated minimum wages, benefits, superannuation and leave entitlements; and
  - (iv) allow workers to freely associate with others, form and join industrial organisations of their choice and engage in any lawful industrial activity without discrimination or retaliation.

## 5.2 Modern Slavery

- (a) Opticomm will not tolerate any form of slavery, forced labour, debt bondage, child labour and human trafficking within its supply chain, including all international elements of the chain.
- (b) Suppliers must:
  - (i) not use any form of forced, bonded or indentured labour;
  - (ii) only employ workers who are of a legal age;
  - (iii) ensure that all work is undertaken without coercion;
  - (iv) ensure that recruitment agencies, if used, are compliant with the provisions of this document and applicable law; and
  - (v) support Opticomm in any other way reasonably required to meet its obligations under the Australian Modern Slavery Act 2018 (Cth).
- (c) Suppliers will respond promptly to any request to complete a supplier Modern Slavery questionnaire or other reasonable questions regarding its work practices.
- (d) Should the Supplier become aware of any Modern Slavery risks or practices in its supply chain or operations, it must:
  - (i) notify Opticomm of those risks and advise Opticomm of the steps it is taking to eliminate or minimise those risks in writing,
  - (ii) immediately notify Opticomm of those practices and of the remediation action it proposes to take; and



- (iii) at its cost, implement remediation action and take any such additional remediation action as may be required by Opticomm acting reasonably.

## 6 Cyber Security and Privacy

### 6.1 Security Policies

- (a) Suppliers must implement industry best practice or technical and organisation security practices that are compliant with Opticomm's security policies. These include protection of customer data and networks from breaches and unauthorised access.
- (b) The policies should be consistent with ISO27001 principles.
- (c) Suppliers must notify Opticomm promptly of any personnel movements, and in particular, must provide notice when Supplier personnel are no longer employed by the Supplier to ensure removal of access to Opticomm's systems. Notice should be given as soon as Supplier is aware that personnel will cease working on Opticomm's project, ideally before the termination date, or if not possible, no more than one Business Day after the event.

### 6.2 Supplier Devices

Devices utilised by Supplier personnel which interact with and/or access Opticomm's systems should, at a minimum:

- (a) not be end of life (EoL) or end of support (EoS) (e.g. a five year old mobile device may no longer receive security updates from the vendor for instance);
- (b) have the latest security and software updates installed;
- (c) not be running any custom ROMS (some android phones can be flashed with custom operating systems);
- (d) be secured by either fingerprint or a password (PIN should not be considered secure, and the quality of face unlock depends on the handset and implementation). Passwords should conform at least to generally accepted password strength requirements, consisting of sufficient length and complexity.

## 7 Notifiable incidents

### 7.1 WHS/OH&S Incidents

The Supplier must notify Opticomm immediately of all accidents, injuries, incidents or near-misses which occur at any premises which result or may result in a risk to health or safety or a breach of WHS/OH&S Legislation

through the Opticomm Incident reporting Portal, (Opticomm Incident reporting Portal) and must provide Opticomm with any assistance, as requested including during an investigation and the provision of a rectification plan or schedule.

## 7.2 Other Incidents

- (a) The Supplier must notify Opticomm:
  - (i) when it becomes aware of Alleged Misconduct or a Serious Incident in relation to the delivery of the Services;
  - (ii) serious complaints received in relation to the delivery of the Services;
  - (iii) the occurrence of any event which may cause adverse publicity to Opticomm or the delivery of Services, or has or may attract significant public interest and attention; or
  - (iv) any current, pending or threatened proceedings which may detrimentally affect Opticomm's reputation or that of its Services.
- (b) The Supplier must immediately notify Opticomm of any incident where Opticomm data is or may be at risk of disclosure to unauthorised parties, including but not limited to:
  - (i) unaccounted loss or theft of any device used to access or store Opticomm data, e.g. phones, laptops, servers, USB drives;
  - (ii) any incident pertaining to unauthorised access to the network, systems or devices used by the company;
  - (iii) becoming aware that any Opticomm data has been handled, stored, shared or used in a manner contrary to these guidelines.