

Workplace Surveillance Policy

SAMPLE

Table of Contents

Purpose and Scope	4
Objectives.....	4
Definitions.....	4
Legal and WHS Framework.....	5
Types of Surveillance Used	5
CCTV and Video Surveillance	5
Computer, Network and Communications Surveillance	6
Tracking Surveillance (Vehicles, Equipment and Devices)	6
Audio Surveillance	7
Other Forms of Surveillance.....	7
Purposes of Surveillance	7
Notification and Signage.....	7
General Notification of Workers.....	7
Signage for CCTV and Audio Surveillance	8
System Owners and Electronic Notices.....	8
Worker and Other Persons' Expectations of Privacy.....	8
Over Surveillance.....	8
WHS Risk Management and Surveillance	9
Role of Surveillance in WHS	9
Integration with WHS Systems.....	9
Use of Surveillance Information	9
Access, Storage and Security of Surveillance Records.....	10
Access Controls	10
Storage and Retention	10
Security Measures	10
Disclosure and Sharing of Surveillance Information	10
Worker Responsibilities	11
Management Responsibilities	11
Consultation, Communication and Training.....	12
Psychosocial Hazards and Surveillance	12

Use of Surveillance in Performance Management and Discipline	12
Personal Devices and BYOD (Bring Your Own Device)	13
Prohibited Conduct Relating to Surveillance	13
Incident Response and Use of Surveillance Evidence	13
Requests for Access to Surveillance Information by Workers.....	14
Implementation Checklist.....	14
Roles and Responsibilities Summary.....	15
Policy Review	15

SAMPLE

Purpose and Scope

This Workplace Surveillance Policy sets out how [Company Name] conducts surveillance in the workplace and in relation to work activities. It is designed to ensure that any surveillance is lawful, reasonable, transparent, and consistent with work health and safety (WHS) obligations, privacy expectations and industrial relations requirements.

This policy applies to: - All workers, including employees, contractors, labour hire workers, apprentices, volunteers and work experience students. - All workplaces controlled or managed by [Company Name], including offices, warehouses, distribution centres, retail stores, manufacturing facilities, workshops, loading docks, and vehicles. - All surveillance systems and technologies operated by or on behalf of [Company Name].

This policy should be read in conjunction with: - WHS Policy and WHS Management System documents - Code of Conduct - Information Security Policy - Privacy Policy - Bullying, Harassment and Discrimination Policy - Enterprise agreements, modern awards and employment contracts where applicable.

Objectives

The objectives of this Workplace Surveillance Policy are to:

- Support [Company Name]'s duty to provide a safe and healthy work environment under WHS legislation.
- Detect and manage unsafe behaviour, misconduct, theft, fraud, and damage to property.
- Protect workers, customers, visitors and members of the public interacting with [Company Name].
- Safeguard company property, stock, equipment, information and systems.
- Ensure surveillance practices are clearly communicated, consistently applied and compliant with relevant workplace surveillance, privacy and WHS laws.
- Balance legitimate business and safety needs with reasonable expectations of privacy.

Definitions

For the purposes of this policy:

- **Workplace surveillance:** Any monitoring, recording, tracking or observing of workers or their activities, communications or locations carried out by or on behalf of [Company Name].
- **CCTV:** Closed Circuit Television systems used to capture video images (and, where enabled, audio) in and around workplaces.
- **Computer surveillance:** Monitoring or recording of the use of computers, networks, email, internet, software, mobile devices and other electronic systems.

- **Tracking surveillance:** Monitoring or recording of the geographical location or movement of vehicles, equipment or devices, including GPS tracking and telematics.
- **Covert surveillance:** Surveillance carried out without prior notification to workers, typically only permitted in very limited circumstances and in accordance with applicable legislation.
- **Overt surveillance:** Surveillance carried out with clear notification to workers, and usually with visible signage or system notices.
- **Worker:** Any person who carries out work in any capacity for [Company Name], including employees, contractors, labour hire, volunteers and others.

Legal and WHS Framework

[Company Name] will conduct workplace surveillance in accordance with relevant Commonwealth, state and territory legislation which may include (as applicable):

- Work Health and Safety Act and Regulation (jurisdiction-specific)
- Workplace surveillance and monitoring legislation (jurisdiction-specific)
- Privacy legislation and Australian Privacy Principles (where applicable)
- Fair Work Act 2009 (Cth) and applicable industrial instruments
- Surveillance devices and listening devices legislation (jurisdiction-specific)

From a WHS perspective, [Company Name] has a primary duty of care to: - Eliminate or minimise risk to health and safety so far as is reasonably practicable. - Provide and maintain safe systems of work. - Monitor conditions at the workplace, including through appropriate use of surveillance where it contributes to risk management.

Surveillance is one of several control measures used to manage WHS risks, particularly in higher-risk environments such as retail and wholesale operations, transport and logistics, and manufacturing and production.

Types of Surveillance Used

CCTV and Video Surveillance

[Company Name] may use CCTV and other video surveillance systems in and around workplaces for purposes including:

- Monitoring and recording activities in areas where safety incidents, aggression, theft, stock loss or equipment damage may occur.
- Supporting incident investigations (e.g. manual handling injuries in a warehouse, forklift collisions in a loading dock, or customer aggression in a retail store).
- Deterring and detecting unlawful activity, misconduct, and breaches of WHS procedures.

Typical locations may include: - Entry and exit points - Retail sales floors, service counters and cash handling areas - Warehousing and storage areas - Loading docks,

dispatch areas and yards - Manufacturing lines and production areas - Car parks and external perimeters - Common areas such as corridors, lifts and reception

CCTV will not normally be used in: - Toilets, change rooms or shower facilities - Designated prayer rooms or similar private spaces - First aid rooms and health consultation areas

Any exception must be justified, risk-assessed, and compliant with applicable laws.

Computer, Network and Communications Surveillance

[Company Name] may monitor the use of:

- Desktop and laptop computers
- Tablets and mobile phones issued by [Company Name]
- Email systems
- Internet and intranet access
- Business applications, including warehouse management systems, transport management systems, point-of-sale (POS) systems, and manufacturing control systems

Monitoring may include: - Log-in and log-out times - Websites visited and duration - Email headers and, where justified, email content - File access, downloads and transfers - Use of removable storage devices - Application usage and transaction logs (e.g. stock adjustments, goods sales, manifest changes)

This surveillance is used to: - Protect confidential and commercially sensitive information. - Maintain system security and detect unauthorised access or malware. - Ensure appropriate use of company systems and compliance with policies. - Support investigations of safety incidents (e.g. reviewing system logs to understand the sequence of events before a warehouse racking collapse or production line stoppage).

Tracking Surveillance (Vehicles, Equipment and Devices)

[Company Name] may use tracking technologies such as GPS, telematics and location services in relation to:

- Company vehicles (e.g. delivery trucks, vans, forklifts, company cars)
- High-value equipment (e.g. trailers, containers, specialised machinery)
- Mobile devices (e.g. smartphones, tablets, handheld scanners) where location services are enabled

Tracking data may be used to: - Manage fatigue and driving hours in transport and logistics. - Monitor speeding, harsh braking and other high-risk driving behaviours. - Verify route adherence and delivery timeframes. - Respond to vehicle breakdowns, incidents or emergencies. - Locate stolen or missing vehicles, equipment or devices. - Support incident investigations following collisions, near misses or unauthorised use.