

Monitoring & Surveillance Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

Workplace surveillance is regulated in some Australian states and territories. In NSW, surveillance must comply with the Workplace Surveillance Act 2005. Similar laws exist in other jurisdictions. Seek legal advice to ensure your monitoring practices comply with applicable legislation.

1. Purpose

This policy informs employees about the monitoring and surveillance practices used by [Company Name]. It ensures transparency, complies with legal requirements and balances legitimate business interests with employee privacy.

2. Scope

This policy applies to:

- All employees, contractors and visitors
- All workplace premises
- All company IT systems and devices
- Company vehicles where applicable

3. Policy Statement

[Company Name] may conduct workplace monitoring and surveillance for legitimate business purposes. We are committed to:

- Being transparent about monitoring practices
- Using monitoring proportionately
- Complying with all legal requirements
- Protecting employee privacy where reasonable

4. Reasons for Monitoring

[Company Name] may conduct monitoring for the following purposes:

- Security of premises, people and assets
- Prevention and detection of theft or fraud

- Health and safety compliance
- Protection of confidential information
- Ensuring compliance with policies
- Quality assurance and training
- Managing IT resources
- Investigating complaints or incidents
- Meeting legal or regulatory requirements

5. Types of Monitoring

5.1 CCTV and Video Surveillance

[Company Name] uses CCTV cameras in the following areas:

- Building entrances and exits
- Car parks
- Reception and public areas
- Warehouse and storage areas
- [Other relevant areas]

CCTV is NOT used in:

- Toilets and change rooms
- Designated private areas
- Areas where there is a reasonable expectation of privacy

5.2 IT Systems Monitoring

[Company Name] may monitor:

- Email communications (business accounts)
- Internet usage and websites visited
- Network traffic and file access
- Software and application use
- Print and copy activities
- Login and access records

5.3 Telephone Monitoring

Where applicable:

- Business calls may be recorded for quality and training
- Call logs may be reviewed
- Callers will be notified of recording where required

5.4 GPS and Vehicle Tracking

If [Company Name] uses GPS tracking in company vehicles:

- Location tracking during work hours
- Vehicle usage monitoring
- Driver behaviour where relevant

5.5 Access Control Systems

- Building access card records
- Entry and exit times
- Access to secure areas

6. Employee Notification

[Company Name] will notify employees about surveillance:

- Through this policy
- Through signage in monitored areas
- In employment contracts and onboarding
- Before new monitoring is introduced

In some states, specific notice requirements apply. [Company Name] will comply with all applicable notification requirements.

7. Privacy Considerations

7.1 Privacy Principles

- Monitoring is proportionate to legitimate purposes
- Only necessary data is collected
- Data is kept secure
- Access to monitoring data is restricted
- Data is retained only as long as necessary

7.2 Limitations

- Monitoring is not used to target individuals unfairly
- Personal communications on personal devices are not monitored
- Monitoring data is not used for unrelated purposes

8. Data Handling

8.1 Access to Monitoring Data

Access to surveillance and monitoring data is restricted to:

- Authorised security personnel

- IT administrators (for IT monitoring)
- Management when investigating specific issues
- HR when required for investigations
- Law enforcement when legally required

8.2 Data Retention

- CCTV footage: [insert period, e.g., 30 days]
- IT logs: [insert period, e.g., 90 days]
- Access records: [insert period]

Data may be retained longer if required for investigations or legal proceedings.

8.3 Data Security

- Monitoring data is stored securely
- Access is logged and audited
- Data is disposed of securely when no longer needed

9. Employee Rights

9.1 Access to Information

Employees may request:

- Information about monitoring that affects them
- Access to footage or records about themselves in some circumstances
- Explanation of how monitoring is conducted

9.2 Raising Concerns

Employees who have concerns about monitoring can:

- Speak to their manager
- Contact HR
- Use grievance procedures

10. Use of Monitoring Information

10.1 Permitted Uses

Monitoring information may be used for:

- Security and safety purposes
- Investigating specific incidents or complaints
- Disciplinary proceedings where relevant
- Legal proceedings
- Providing evidence to law enforcement

10.2 Prohibited Uses

- General surveillance of employees without cause
- Sharing data externally except as permitted
- Using data for purposes unrelated to the reasons for collection

11. Covert Surveillance

Covert surveillance (surveillance without employee knowledge) will only occur:

- Where there is reasonable suspicion of unlawful activity or serious misconduct
- Where overt surveillance would be ineffective
- In compliance with legal requirements
- With appropriate authorisation

12. Legal Compliance

[Company Name] will comply with:

- Workplace surveillance legislation in applicable states
- Privacy Act 1988 and Australian Privacy Principles
- Telecommunications legislation
- Any other relevant laws and regulations

13. Responsibilities

13.1 Management

- Ensure monitoring is conducted appropriately
- Authorise access to monitoring data
- Investigate concerns about monitoring

13.2 IT/Security

- Implement and maintain monitoring systems
- Ensure data security
- Provide data when properly authorised

13.3 Employees

- Be aware of monitoring practices
- Comply with policies
- Raise concerns through appropriate channels

14. Review

This policy will be reviewed:

- At least annually

- When monitoring practices change
- When legislation changes
- When concerns are raised

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s Monitoring & Surveillance Policy. I understand that workplace monitoring may occur as described in this policy.

Employee Name: _____

Signature: _____

Date: _____