Closed Circuit Television Policy

Last Review Date:	July 2019
Next Review Date:	July 2022
Approved by:	Integrity Governance Committee; July 2019
Owner:	General Manager Health, Safety and Security

Purpose

The purpose of this policy is to cover the Ministry's use of Closed Circuit Television (CCTV) for the protection of people, property and to ensure that this does not unreasonably impinge on people's rights.

Policy Statement

The Ministry is committed to providing a safe environment for staff, clients and visitors.

CCTV is a security control that forms part of the MSD Security Eco-System (refer Appendix 1). MSD has developed the security eco-system in accordance with:

- Health and Safety at Work Act 2015;
- Industry best practice; and
- NZ Government Protective Security Requirements (PSR).

The security eco-system provides a multi-layered system of security measures that matches the security risks facing our people. This means that if a single layer of security is breached, there are additional layers of protection in place to minimise harm.

CCTV is used as a security measure to:

- deter criminal activity
- enable a response to real time threats, and
- for evidentiary purposes:
  - in MSD investigations
  - investigations by other New Zealand Government agencies in pursuit of their lawful duties.

MSD has organisational safeguards in the form of business processes and procedures to ensure compliance with this policy, including guidance on the use, storage and disclosure of any retained CCTV imagery.

Scope

In Scope

This policy applies to the Ministry's use of CCTV at its offices, including both internal and external coverage.

This includes offices where the Ministry is co-located with other agencies, in the following situations:

- MSD is the lead tenant and operates the CCTV
- MSD is not the lead tenant and the other agency operates the CCTV.

CCTV imagery that is retained or live streamed without retention.

Services and responsibilities provided by contracted third parties pertaining to Ministry CCTV systems.

Appropriate use and disclosure of CCTV information.

Out of Scope

Covert cameras that are installed as part of an investigation into fraud, theft or property damage.

Policy requirements

The Ministry will ensure that it complies with the following when using CCTV:

- Health and Safety at Work Act (HSWA) 2015
- New Zealand Bill of Rights Act (BORA) 1990
- New Zealand Government Protective Security Requirements (PSR)
- Privacy Act 1993
- Privacy Commissioner: Privacy and CCTV Guidelines 2009
- MSD Code of Conduct
- State Services Commission Code of Conduct

The Ministry will require staff and contractors to comply with the following:

- CCTV information is only used for the purpose it was collected, to manage the identified risk
- Appropriate access management is in place to ensure only the relevant staff / contractors have access to the CCTV information
- A business process that describes how information is to be used and protected
- Training is provided to staff / contractors to ensure the information is used and protected appropriately
- Answer queries from people (including clients) about the Ministry's use of CCTV.

Policy principles

- We are transparent about our use of CCTV.
- In our determination to use CCTV in Ministry offices we will consider the following aspects:
    - whether it is necessary and proportionate to manage the identified risk and that it is fit for purpose.
    - which risks CCTV is being used to manage
    - where CCTV system components should be installed to ensure coverage is appropriate
    - whether the information collected by the camera will be retained or live streamed without retention
    - whether the camera allows a person to be identified or observed.
- We control access to ensure that information is used appropriately by staff / contractors

- We provide access to CCTV information to people when they request it in compliance with the Privacy Act 1993.
- Where we record CCTV information we store the information only for as long as is reasonably required to manage the identified risk.
- We ensure the appropriate retention, use, storage and disclosure of any retained CCTV imagery through written business processes and procedures.
- All layers of the security eco-system are inter-related and the CCTV security measure will form part of regular reviews of the security eco-system.

Responsibilities

(Specific and general responsibilities of staff to ensure compliance with the policy)

Person/Party	Responsibilities
Leadership Team	Officers responsibility under the HSWA and for the security eco-system for the Ministry.
Chief Security Officer (CSO)	Is the accrediting authority for CCTV systems (may be delegated).
Chief Privacy Officer (CPO)	Is the authority for how the Ministry meets its obligations under the Privacy Act.
Chief Information Security Officer (CISO)	Is the accrediting authority for information security and ensures our applications and systems meet the Ministry's security requirements.
Health Safety and Security Team	Responsible for compliance of the CCTV configuration with the CCTV policy.
Managers at MSD offices	Responsible for controlling access to any retained CCTV imagery including the release of any retained imagery requested by an appropriate authority for lawful purposes, e.g. NZ Police.

Definitions

(Explanation of terms used in the policy and in fulfilling responsibilities in the policy)

Word/ phrase	Definition
MSD offices	Includes all sites, e.g. Regional Offices, Service Centres, National Office, co-located offices with other tenants.
Public Spaces	Areas within an MSD office where there is public access and external spaces.

Systems components	Includes the items that enable operation of the CCTV, e.g. camera, monitor, server.

Related policies

(List the Department's other policies that should be referred to in conjunction with, or support, this one)

Policy	Owner
Health and Safety Policy	General Manager, Health Safety and Security
Privacy Strategy	Associate DCE, Corporate Solutions
Information Gathering Oversight Policy	General Manager Information Group

Appendices

- **Appendix 1:** Security eco-system