

State Library of New South Wales
Security Systems Surveillance Policy

Approved by: Executive Committee	
File Number: 30675	Review Date: May 2014
Policy Owner: Director, Operations and CFO	
Contact Person: Manager, Facilities & Security	
Brief description: Policy to manage use of security systems and surveillance equipment for protection of State Library collections and premises and the safety of staff, and visitors.	
Related policies: Code of Conduct; Collection & Services Disaster Response Plan; ICT Services Policy; Information Security Policy; OHS Policy; Privacy Management Plan;	
Supersedes: Policy Controlling the Use of Security Systems, version 5, 2004; Access Control Policy	
Document Version: 6.0	

Introduction

The State Library of NSW collects, maintains and preserves items of historical importance on behalf of the people of New South Wales. As custodian of these objects the State Library has a role in providing public access to them. It is the responsibility of the State Library to provide a safe and secure environment for collection material, visitors and clients and staff. The Mitchell Library is a heritage building that the State Library maintains and protects for the Government and people of New South Wales.

State Library security systems provide controlled access to sensitive areas and surveillance of State Library environs, contributing towards this safe and secure environment. The security systems:

- act as a deterrent, reducing the likelihood of theft or damage to Library collections or property, and of aggressive or inappropriate behaviour towards staff, clients and visitors
- permit real-time monitoring, allowing Security Staff to respond quickly and effectively to incidents
- provide a record of events which may be used to identify perpetrators and support evidence provided by witnesses.

Policy Statement

This policy identifies the security systems used at the State Library and describes how they are used, in accordance with the *Workplace Surveillance Act 2005* and other relevant legislation and policies.

This policy applies to all persons within the State Library's precinct.

Legislative and Policy Framework

Most relevant legislation:
Crimes Act 1990

Library Act 1939
Library Regulation 2010
Occupational Health and Safety Act 2000
Privacy and Personal Information Protection Act 1998
Public Sector Employment and Management Act 2002
Workplace Surveillance Act 2005

Related State Library policies:

Client code of Conduct
Code of Conduct
Collection & Services Disaster Response Plan
Use of the State Library Under the Library Regulation 2005 Part 3
Information and Communications Technology (ICT) Services Policy
Information Security Policy
Occupational Health and Safety Policy

This policy supports the State Library's information security management framework under standard AS/NZS ISO/IEC 27001:2006 and meets the requirements of the Library's *Privacy Management Plan*.

Policy

This policy covers the security systems including camera, and tracking surveillance at the State Library. Computer, internet and email surveillance is covered by the ICT Services Policy.

The following security surveillance systems are in place at the State Library:

- Closed circuit television (CCTV) cameras, with video recording equipment
- Cardax Access Control Monitoring and Reporting
- Cardax Security Alarm Monitoring System (including Passive Infrared Detectors (PIRs) and Reed Switch sensors).
- Photographic identification cards
- Visitor contractor attendance kiosk

Surveillance from all security systems is continuous and ongoing, 24 hours per day, 7 days per week.

Surveillance is not used to monitor employees' work performance.

Surveillance of change rooms and bathrooms is prohibited.

Printouts from the Alarm Monitoring System are used to:

- monitor and investigate incidents, such as an unauthorised access or where there is considered to be reasonable suspicion of corrupt practice or illegal activity, and
- confirm that Security patrols are taking place.

Where there is considered to be reasonable suspicion of corrupt practice or illegal activity, the Manager, Facilities & Security may seek authorisation from a Magistrate for covert surveillance.

Computers connected to the Security network are used solely for monitoring alarm points and Cardax access via ID cards.

CCTV Cameras

1. The State Library is equipped with both internal and external CCTV cameras, positioned at various locations throughout the Library complex, and connected to video image recording equipment.
2. CCTV cameras provide Security staff with the means to monitor multiple areas of the State Library at any one time and allow them to monitor activities around the site without exposing themselves to personal danger.
3. CCTV cameras are visible to staff and visitors. Details of the types and locations of the fixed State Library cameras are in Attachment One.
4. Signage has been installed at appropriate points to inform staff and the public of the presence of security surveillance cameras with recording capability. Details of sign locations and a copy of the signage currently used are in Attachment One.
5. Additional CCTV cameras may be installed under certain circumstances and in accordance with this policy, including:
 - new exhibitions: to cover specific objects of high value or importance or in areas considered to contain potential risks
 - perceived risks: to either the State Library's collections or its staff, or to visitors, or to areas within the buildings.
6. CCTV cameras may be used to track the movements of members of the public where there is reasonable suspicion of a threat or risk to the security of the State Library or other people within the Library precinct.
7. Cameras are operated from the Security Control Room and are only used for the maintenance of security within the State Library and around the State Library's perimeters. Only authorised staff, with the appropriate Security Licence, may operate camera equipment.

Video Recording

1. The State Library undertakes continuous and ongoing recording of visual images from certain CCTV cameras, recording the time and date at which images are taken.

2. Security staff are able to sequence through CCTV cameras located throughout the site for monitoring purposes only. Access to video recording equipment is restricted to authorised staff only.
3. Images are recorded on a hard disk and are retained for up to 2 months. Overwriting of the disk commences after 2 months.
4. Recorded images are not available to members of the public.
5. Access to recorded images by Library staff is limited. The Manager Facilities & Security, in consultation with the Director, Operations, may approve the release of still images from video images to staff in order to alert them to possible risks or obtain their assistance in identification.
6. In some circumstances, the Manager, Facilities & Security, in consultation with the Director Operations, may approve the copying of a recorded incident which is then set aside in a secure cabinet. These circumstances include:
 - where there is footage of an incident with the potential to result in a breach of Library Regulation 2010, or is subject to legal proceedings or a civil claim
 - as a result of a reasonable request from a solicitor (pending a court order for the release of the footage).
7. Video recordings of a specific incident may be released to the NSW Police Service only under the terms of this policy or subject to the execution of a search warrant or other legal process and only with the approval of the State Librarian & Chief Executive, a member of the Executive or a Senior Manager, in consultation with the Library's Privacy Contact Officers.

Photographic ID Cards

1. All staff, volunteers and contractors must wear a State Library Identification card or pass at all times when onsite.
2. Staff must challenge/query or report immediately to security anyone seen in non-public areas without an ID card or temporary pass.
3. The digitised photographs are maintained within the Cardax Security System. The following information is stored with the digitised image, within the same database:
 - name
 - division, branch, section
 - nature of employment (permanent/temporary/volunteer etc)
 - date of card issue
 - expiry date of card
 - building access level.

4. Information maintained within this database is available only to Security staff and the photographic images may not be issued to anyone other than the individual.
5. The database is backed up in accordance with the ICT Services Policy.

Cardax Access Monitoring and Reporting

1. The Cardax system collects and stores information on the time and date a personal ID was swiped in a particular Cardax reader.
2. Reports on access to areas of the Library may be produced by either individual card number or by area under the following circumstances:
 - for individual cards, only with the approval of the Manager, Facilities & Security where there is reasonable suspicion of improper use/conduct, or for example, to trace a lost card.
 - in the event of an incident to determine who may have accessed the area. and/or
 - as part of a regular review of access to an area e.g. staff offices.

Cardax Access Control Security Alarm Monitoring

1. The Access Control Security Alarm System uses door alarm devices and passive infra-red detectors to monitor the State Library site. When these devices are triggered, an alarm sounds and Security staff are alerted.
2. The system records the location of the alarm and the time and date when it was triggered. This information is stored locally on the Cardax System and can only be accessed by authorised staff.

Accountabilities

The State Librarian and Chief Executive is accountable for: approving this policy and for authorising the release of video footage, in accordance with this policy.

The Executive is accountable for ensuring that this policy: meets all legislative requirements; is implemented and regularly reviewed; and is communicated to managers and supervisors.

The Manager, Facilities & Security is accountable for: managing the State Library's security systems; ensuring that all complaints about breaches of this policy are investigated and appropriate action taken; and monitoring the work practices of Security staff. The Manager, Facilities & Security is responsible for updating and implementing this policy.

The Security Coordinators are responsible for: administering the installation and maintenance of all security systems and surveillance equipment; and for advising on the review and amendment of this policy. Security Coordinators are also accountable for monitoring and reporting on security breaches.

Security staff are responsible for: advising on the review and amendment of the security surveillance policy as required; . Security Coordinators are also accountable for monitoring/reporting breaches

Managers and supervisors are accountable for: ensuring their staff understand and comply with the requirements of this policy; and notifying the Manager Facilities & Security or a Security Coordinator as soon as practicable whenever their staff report an incident.

Staff are accountable for: understanding and complying with this policy; and must report any security incidents or breaches of this policy to the Manager, Facilities & Security or a Security Coordinator.

Reporting requirements

The Manager, Facilities & Security will report to the Executive on any breaches of this policy.

Approval

This policy was approved by the Library's Executive Committee on 23 May 2011.

Implementation

This policy is implemented on 24 May 2011.

Review

The policy will be reviewed in May 2014.

History

This policy replaces the *Policy Controlling the Use of Security Systems* and the *Access Control Policy*.

Contact

For further information on this policy contact the Library's Manager, Facilities & Security or Security Coordinators.

Reviewed by:

Manager, Facilities & Security

28 October, 2010

and

Security Coordinator

12 May 2011

Attachment One:

Types and Locations of CCTV Cameras

Approximately 140 fixed cameras are installed within the State Library buildings and environs. . Several security cameras have the capacity to be panned, tilt & zoomed (PTZ).

The system is monitored [REDACTED].
[REDACTED]. The system can also be monitored remotely from the following locations:

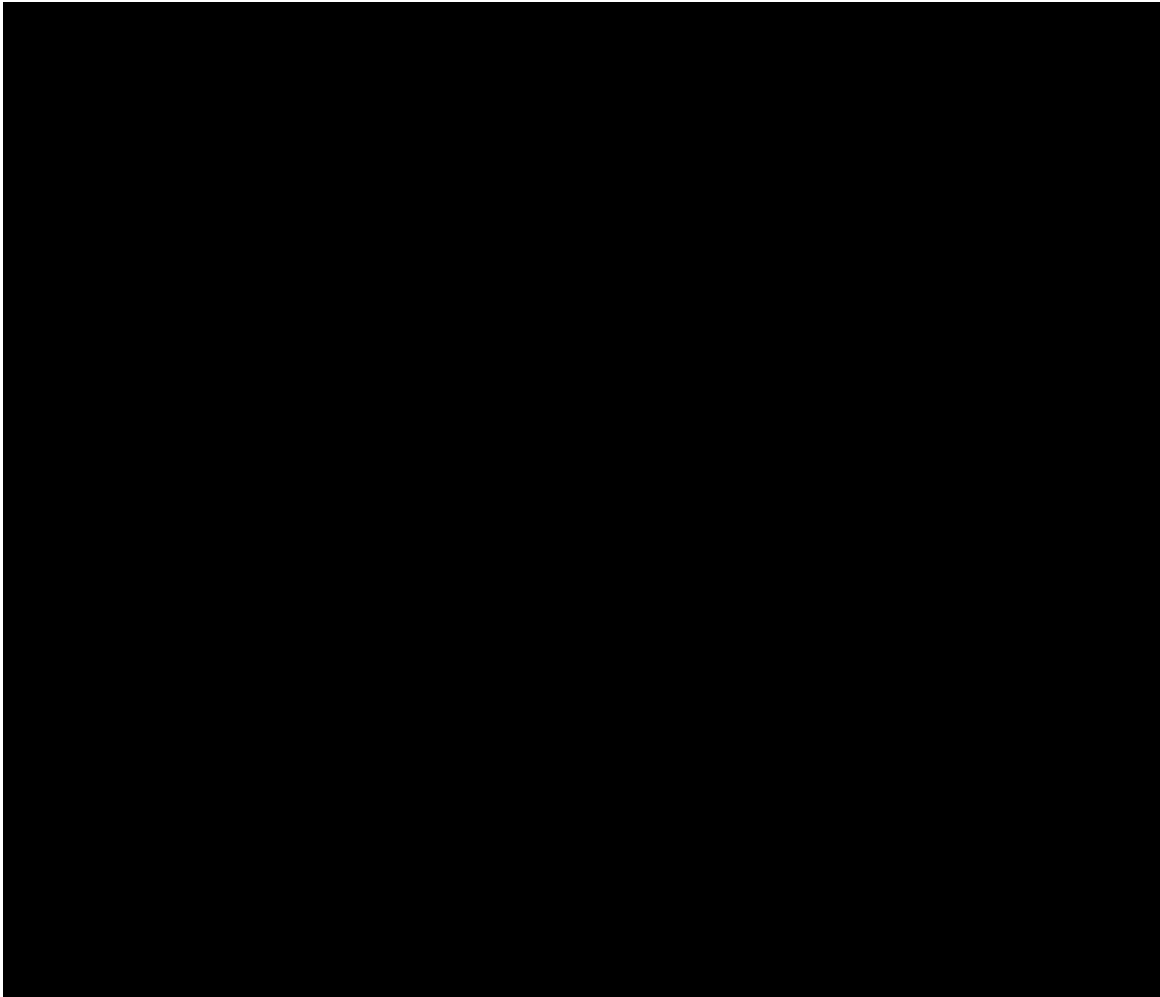
- [REDACTED]
- [REDACTED].

A digital image recording system has been installed and connected to record images from specific cameras.

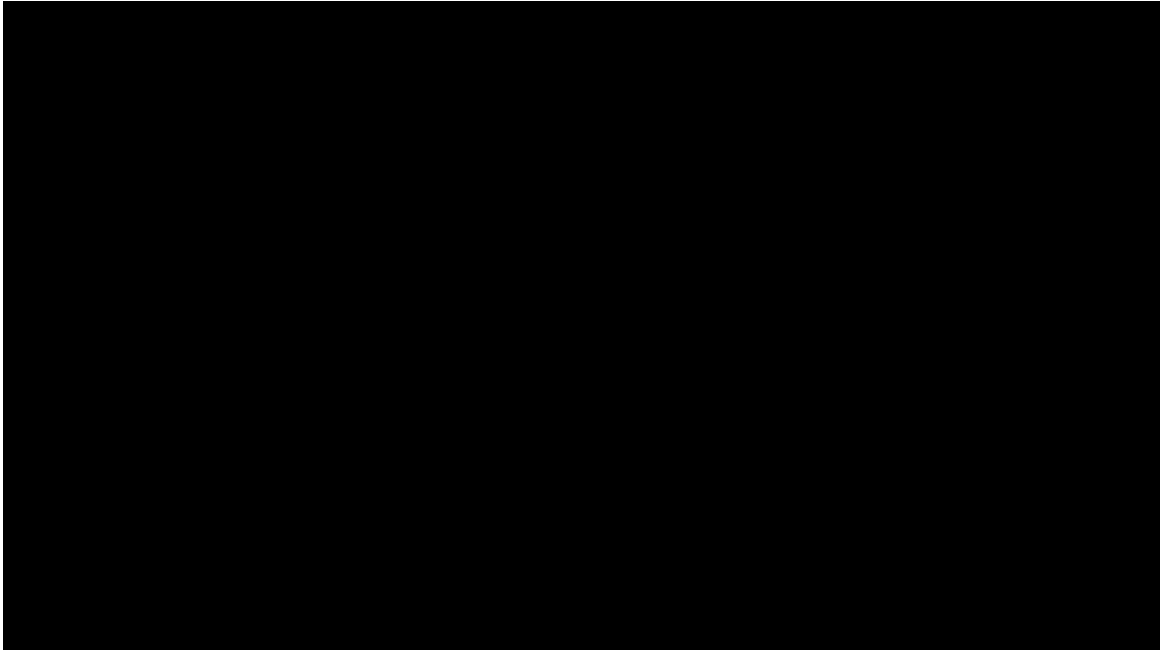
Location of Cameras Connected to Video Recording Equipment

Cameras connected to digital recording equipment are located as follows:

Macquarie Street Wing Cameras



Mitchell Wing Cameras



Signage – Location and Wording

Signage has been installed at all entrances to the State Library premises and in all rooms where CCTV cameras have been installed. The signs inform staff and the public of the presence of security surveillance cameras with recording capability.

Wording of Signage

For your safety and the security of the collections, this library complex is monitored by closed circuit television linked to visual image recording equipment.

