

Security Systems Surveillance Policy



Version: 1.0

Last Amendment:

Approved by: Executive

Policy owner/sponsor: Director, Operations and CFO

Policy Contact Officer: Manager, Facilities & Security

Policy No: PD/33 TRIM File No: 43427

Date approved: 03/12/2013

Next review: 03/12/2016

1. Summary

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.

2. 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.

3. Legislative and Policy Framework

Most relevant legislation:

- *Crimes Act 1990*
- *Government Information (Public Access) Act 2009*
- *Library Act 1939*
- *Library Regulation 2010*
- *Privacy and Personal Information Protection Act 1998*
- *Public Sector Employment and Management Act 2002*

- *State Records Act 1998*
- *Work Health and Safety Act 2011*
- *Workplace Surveillance Act 2005*
- *Workplace Surveillance Regulation 2012*

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 2010 Part 3
- Information and Communications Technology (ICT) Services Policy
- Information Security Policy
- Privacy Management Plan
- Records Management Policy
- Work Health and Safety Policy

This policy supports the State Library's information security management framework under standard AS/NZS ISO/IEC 27001:2006 and AS/NZS ISO/IEC 27002:2006.

4. 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
- Gallagher Access Control Monitoring and Reporting
- Gallagher Security Alarm Monitoring System (including Passive Infrared Detectors (PIRs) and Reed Switch sensors)
- Photographic identification cards
- Kwiklook Data-Base & 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 unauthorised access or where there is considered to be reasonable suspicion of corrupt practice or illegal activity.

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

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

4.1 CCTV Cameras

- a. 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.
- b. 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.
- c. CCTV cameras are visible to staff and visitors. Details of the types and locations of the fixed State Library cameras are in Attachment One.
- d. 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.
- e. 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.
- f. 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.
- g. 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.

4.2 Video Recording

- a. 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.
- b. 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.
- c. Images are recorded on a hard disk and are retained for up to 14 days. Overwriting of the disk commences after 14 days.
- d. Recorded images are not available to members of the public. Access to recorded images by Library staff is limited.
- e. The Manager, Facilities & Security, in consultation with the Director, Operations & CFO, 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.

- f. The Manager, Enterprise Information or the Privacy Contact Officer in consultation with the Director Operations & CFO and the Security Controller, 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 that may be subject to investigation or 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).
- g. Video recordings of a specific incident may be released to the NSW Police Service or other law enforcement agency, subject to the execution of a search warrant or where another Act or law authorises or requires us to do so and, only with the approval of the NSW State Librarian & Chief Executive or delegate, in consultation with the Manager, Enterprise Information or the Privacy Contact Officer. Refer to the CCTV footage release procedure on the Intranet.

4.3 Photographic ID Cards

- a. All staff, volunteers and contractors must wear a State Library Identification card or pass at all times when onsite.
- b. Staff must challenge/query or report immediately to security anyone seen in non-public areas without an ID card or temporary pass.
- c. The digitised photographs are maintained within the Gallagher 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.
- d. Information maintained within this database is available only to Security staff. Photographic images may not be used for any other purpose, or disclosed to any other person or body, without the consent of the individual to whom the information relates or unless another Act or law authorises or requires us to do so.
- e. The database is backed up in accordance with the ICT Services Policy.

4.4 Gallagher Access Monitoring and Reporting

- a. The Gallagher system collects and stores information on the time and date a personal ID was swiped in a particular Gallagher reader.
- b. 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.

4.5 Gallagher Access Control Security Alarm Monitoring System

- a. This 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.
- b. This system records the location of the alarm and the time and date when it was triggered. This information is stored locally on the system and can only be accessed by authorised staff.

4.6 Kwiklook Data-Base & Visitor-Contractor Attendance System

- a. The Kwiklook Data-Base is used to record all occurrences that occur on-site during a 24hour period. This information is entered manually by Security staff and is stored on the State Library SQL Network Database. This information can only be accessed by authorised staff.
- b. Kwiklook Tours Patrol Recording Device is used by Security staff when performing after-hour building patrols. This device is used to confirm that Security patrols are taking place.
- c. The Kwiklook visitor and contractor attendance kiosk is used to record the arrival and departure times of all visitors and contractors that visit the State Library. The system captures basic contact details and issues an adhesive photo identification pass.

5. Responsibilities

The NSW State Librarian & 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 Controller 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 Controller 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.

The Manager, Enterprise Information and/or the Privacy Contact Officer are responsible for: approving the copying of a recorded incident; and for processing all requests from the NSW Police Service or other law enforcement agency for the release of footage from CCTV cameras.

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 Controller as soon as practicable whenever their staff report an incident.

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

6. Privacy

The privacy and personal information pertaining to security systems surveillance is maintained and managed in accordance with the requirements of the *Privacy and Personal Information Protection Act 1998* and the Library's Privacy Management Plan and procedures.

7. Right to Information

Under some circumstances, information pertaining to security systems surveillance may be released, subject to consultation, in response to an application request made in accordance with the *Government Information (Public Access) Act 2009*.

8. Recordkeeping

Full and accurate records of all activities regarding surveillance such as monitoring or investigating incidents, authorising copying of footage or processing requests from law enforcement agencies are to be maintained securely and are to be registered in the State Library's recordkeeping system in accordance with the Records Management Policy and the *State Records Act 1998*.

9. Reporting requirements

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

10. Approval

This policy was approved by the Executive on 4 December 2013.

11. Implementation

This policy is implemented on 16 December 2013.

12. History

This policy replaces Security Systems Surveillance Policy 2011.

13. Prepared by:

Security Coordinator
2 December 2012

14. Document History and Version Control

Version	Date approved	Approved by	Brief description
1.0	16 December 2013	Executive	First release

Attachment One:

CCTV Cameras

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

The CCTV system is monitored [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

[REDACTED]

Mitchell Wing Cameras


[REDACTED]

[REDACTED]

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.

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



For your safety and the safety of the collections, the library is **monitored by closed circuit television** linked to video recording equipment.



PSG 0961-0003

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

January 2003

PSG 0176-11-0003