Sydney Opera House Policy

Title:	Camera and Access Surveillance Policy
Policy Number:	SOH138
Effective Date:	6 September 2017
Authorisation:	Chief Executive Officer
Authorisation Date:	6 September 2017
Superseded Policy:	SOH138
Accountable Director:	Director, Building, Safety & Security
Responsible Officer:	Head of Security, Emergency Planning & Response

1. CORE PROPOSITION

1.1 The Opera House uses camera and access surveillance systems to support its duty to provide a safe and secure environment.

1.2 This Policy sets out the purpose of the Opera House's camera and access surveillance systems, broadly identifies the location of closed circuit television (**CCTV**) and other camera and access surveillance, and describes how surveillance data is stored, how long it is retained and in what circumstances the Opera House will allow access to the data.

Notice to employees

1.3 This Policy is notice to all employees of workplace surveillance, as required by the *Workplace Surveillance Act 2005* (**WS Act**). Camera and access surveillance are carried out by authorised officers on an ongoing, continuous basis at Sydney Opera House Premises in accordance with this Policy.

1.4 Neither camera nor access surveillance is permitted at the Sydney Opera House premises unless undertaken by authorised officers in accordance with this Policy. Recording people's images or voices without consent may be illegal and may also amount to misconduct

2. SCOPE

2.1 This Policy applies to all Sydney Opera House employees (including permanent, temporary and casual employees), contractors and persons otherwise engaged to undertake work on behalf of the Opera House.

2.2 This Policy also applies to business partners, presenting partners, performers and visitors to Sydney Opera House Premises.

3. DEFINITIONS

3.1 **Access surveillance** – the creation, monitoring, collection and use of records about access to and within Sydney Opera House Premises.

3.2 **Authorised officers** – users who, as part of their duties and responsibilities, are required and authorised to access surveillance data, but only to the extent required to fulfil those duties and responsibilities.

3.3 **Camera surveillance** – the creation, monitoring, collection, storage and use of data obtained through closed circuit television (CCTV) and other image capture systems on the Sydney Opera House premises, and the operation and maintenance of those systems.

3.4 **Surveillance data** – for the purposes of this policy means information collected through the camera and access surveillance systems by or on behalf of the Opera House.

3.5 **Sydney Opera House premises** – includes internal and external areas of the Sydney Opera House building and precinct administered by the Sydney Opera House Trust. It also includes all other premises occupied by the Sydney Opera House Trust from time to time, including offices at Pitt Street and warehouse facilities at St Peters and Leichhardt, or any other premises at which Sydney Opera House employees undertake their duties. It includes building entrances and exits, foyers, lift wells, hallways, theatres (including the stage), service counters, food and beverage areas and vehicle access areas.

4. PURPOSE OF CAMERA AND ACCESS SURVEILLANCE

4.1 The Opera House's camera and access surveillance systems are part of an organisation-wide approach to safety and security management that also includes physical security presence, access control within and to the Sydney Opera House premises, monitoring and alarms.

4.2 The Opera House operates camera and access surveillance for the following purposes:
- To enhance the safety and security of the Opera House;
- To protect the reputation of the Opera House;
- To monitor compliance with rules, policies and procedures;
- To investigate claims, accidents, incidents and breaches of the law, or allegations of such, and for the purpose of any relevant legal proceedings; and
- For audit and reporting purposes.

5. LOCATION OF CAMERA AND ACCESS SURVEILLANCE

5.1 A number of overt CCTV cameras are located in the Sydney Opera House premises.

5.2 CCTV cameras will as far as possible be clearly visible and not deliberately hidden, while always being respectful of the Opera House's heritage obligations as embodied in the Opera House's Conservation Management Plan. Appropriate signage notifies all persons entering the Sydney Opera House Premises that CCTV cameras are in use.

5.3 The Head of Security, Emergency Planning and Response will consult with relevant business units should there be a requirement to install new CCTV cameras in the vicinity of their work area. Staff will be notified of any such installations in accordance with the WS Act.

5.4 Persons authorised under the *Sydney Opera House Trust By-law 2015* may take photographs or make other forms of images of a person where they suspect on reasonable grounds that the person is:
- Contravening or has contravened any provision of the Opera House's By-law; or
- Committing or has committed any other offence on the Sydney Opera House Premises.

5.5 Camera surveillance will never be carried out in change rooms, dressing rooms, toilets and showers.

5.6 Access surveillance occurs wherever swipe cards and cyber keys are used.

6. MONITORING AND STORAGE OF SURVEILLANCE DATA

6.1 Monitoring of surveillance data is undertaken continuously in the Security Control Room (SCR), and in other locations as required. However, not all CCTV cameras are continuously monitored.

6.2 Surveillance data is recorded and stored on hard drives in a secure data centre inside the Sydney Opera House premises. Hard copies of camera surveillance data may also be securely held from time to time.

6.3 The exceptions to the above are a small number of live audio and video feeds that are used for event and safety management. These include feeds from foyers and public areas to stage managers' desks; stage views broadcasts; and feeds monitoring Loading Dock traffic. These feeds are not recorded and stored for the purposes identified in 4.2.

7. RETENTION AND DISPOSAL OF SURVEILLANCE DATA

7.1 Generally, camera surveillance data will be deleted or over-written within 90 days of recording, unless it is required in relation to security or safety incidents, an investigation, inquiry, claim or legal proceedings, in which case retention and disposal requirements apply as specified for video and visual surveillance records in the *NSW State Records General Retention and Disposal Authority*.

7.2 Surveillance data will be managed in accordance with the requirements of the *Privacy and Personal Information Protection Act 1998* (NSW) and other relevant legislation and policies relating to the control of personal information, including the Opera House's *Privacy Management Policy and Plan*.

8. ACCESS TO SURVEILLANCE DATA

8.1 Access to surveillance data is controlled by the Head of Security, Emergency Planning and Response and the Director, Safety, Security and Policy.

8.2 Requests for access to surveillance data must be made in writing to the Head of Security, Emergency Planning and Response, or the Director, Safety, Security and Policy, clearly outlining the reason for access and under what authority the request is being made.

8.3 Surveillance data may be made available to Opera House employees and third parties for any purpose authorised by law, for example:

- To the Sydney Opera House Trustees; members of the Executive; or an appropriate supervisor;
- To a law enforcement agency or other government agency;
- Where required or permitted under the *Government Information (Public Access) Act 2009* (see the *SOH Access to Information (GIPA) Policy* for more information);
- Where required or permitted under the *Privacy and Personal Information Act 1998* (NSW) (see the *SOH Privacy Management Policy and Plan* for further information); or
- To meet a legal requirement (such as a subpoena).

9. RESPONSIBILITIES

9.1 **Authorised officers** are responsible for:

- Protecting the integrity of camera and access surveillance, and preventing improper disclosure of data;
- Undertaking their duties in accordance with this policy, relevant standard operating procedures and training; and
- Reporting any breaches, or suspected breaches, of this Policy to the Duty Security Manager (DSM).

9.2 The **Head of Security, Emergency Planning and Response** is responsible for:

- Monitoring use and performance of camera and access surveillance, including associated audits, risk assessments and policy compliance; and
- The implementation and review of this Policy.

10. SUPPORTING DOCUMENTS AND RELEVANT LEGISLATION

Workplace Surveillance Act 2005
Surveillance Devices Act 2007
Privacy and Personal Information Protection Act 1998
Sydney Opera House Trust By-law 2015
SOH Acceptable Information and Technology Use and Surveillance Policy
SOH Access to Information (GIPA) Policy
SOH Code of Conduct
SOH Privacy Management Policy and Plan
NSW General Retention and Disposal Authority
Australian Security Industry Association CCTV Code of Ethics

APPROVED

Chief Executive Officer
Date: 6 September 2017