Closed Circuit Television (CCTV) Policy

Document Management

Title:	Closed Circuit Television (CCTV) Policy		
Policy Number:	SOH138		
Effective Date:	3 August 2012	**Next Review:**	August 2014
Authorisation:	Chief Executive		
Authorisation Date:	31 July 2012		
Superseded Policy:	N/A		
Accountable Director:	Director, Building Development and Maintenance		
Responsible Officer:	Head of Security, Emergency Planning and Response		

Version Control

Version	Date	Author	Approval	Details/Comments
1.0	June 2012	BDM/Corporate		Draft 1

Contents

1 Purpose

This policy sets out requirements for the management and use of Closed Circuit Television (CCTV) systems on Sydney Opera House premises.

2 Scope

This policy applies to all Sydney Opera House staff, including contractors and other service providers, as well as business partners, presenting partners, performers, visitors and other guests.

This policy has particular application to security officers and other authorised officers required to operate, manage or otherwise required to deal with CCTV systems, equipment or information.

Any proposed amendments to the conditions or procedures in this policy and any associated documents require the review and authorisation of the Head of Security, Emergency Planning and Response.

3 Definitions

Operating Staff – all Sydney Opera House staff authorised to access and operate CCTV systems on a regular basis as approved by the Head of Security, Emergency Planning and Response.

Recorded material – includes all images and data recorded by Sydney Opera House CCTV systems, including original and copies of video recordings and still photographs.

4 Policy

4.1 System Purpose

4.1.1 Sydney Opera House has established CCTV systems in order to support the maintenance of a safe and secure environment for staff, customers, visitors, business and presenting partners and guests. CCTV also assists with the security of assets by acting as a deterrent against acts of vandalism and theft.

4.1.2 CCTV is used as part of an organisation-wide approach to security management that includes a variety of strategies, systems and facilities such as physical security presence, access control, monitoring and alarms.

4.1.3 CCTV systems and collection of recorded material/information from those systems will be managed in accordance with relevant legislation, regulations and Sydney Opera House policies and procedures including the *Workplace Surveillance Act 2005* (NSW).

4.1.4 Only systems and equipment approved by the Head of Security, Emergency Planning and Response will be used on the Sydney Opera House site. Cameras and associated equipment will only be installed in areas permitted by the Head of Security, Emergency Planning and Response with regards to legal, security and site specific requirements.

4.2 System Details

4.2.1 The system consists of a number of overt CCTV cameras situated on Sydney Opera House premises, which continuously record activities in these areas. In general CCTV cameras will be limited to public areas such as the exterior visitor precinct, building entrances and exits, foyers, hallways, commercial outlet areas and vehicle access areas.

4.2.2 With consideration of the State, National and World Heritage status of the building, CCTV cameras will not be hidden and as far as possible be within public view. Appropriate signage will be established to notify all persons entering or within Sydney Opera House premises that CCTV cameras are in use.

4.2.3 The Emergency Planning and Response Group (EPRG) 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 *Workplace Surveillance Act 2005*.

4.2.4 Dedicated facilities with restricted access receive footage from cameras which is recorded and stored in the security data centre room. Access to the security data centre room is controlled by swipe card. The security personnel can access recorded material stored in the security data centre from the primary security control room. The control room is staffed by appropriately authorised security officers and is equipped with communications and information systems to coordinate Emergency Planning and Response incidents and maintain site integrity in response to CCTV footage.

4.3 Access to Systems

4.3.1 Access to CCTV systems, whether to operate equipment or view recorded material is strictly limited to appropriately trained and authorised officers as approved by the Head of Security, Emergency Planning and Response.

4.3.2 Staff from the Sydney Opera House security maintenance contractor Comvision may enter the control room, security equipment room and the security secondary control room located on the lower concourse without formal approval, provided it is for security maintenance work. If they require access for external clients, approval must be obtained from the Head of Security, Emergency Planning and Response.

4.3.3 Approval for and control of access to recorded material or information is restricted to the Head of Security, Emergency Planning and Response. Information and recordings will not be made available to third parties except in the following circumstances:

- To assess or investigate an occupational health and safety incident, hazard or other complaint.
- To identify and investigate an unlawful act, security breach or suspected criminal conduct (incl. referral to NSW Police).
- To ensure security and safety policies are being observed.
- To monitor access to premises and to detect unauthorised access.
- In the course of an investigation into staff misconduct or disciplinary proceedings;
- For training purposes and pre-planned emergency/security operations where permitted and prior approval is obtained.
- Where required to meet a legal requirement.

4.3.4 Requests for third party access to recorded material must be made to the Head of Security, Emergency Planning and Response, clearly outlining the reason for access in accordance with the circumstances listed in 4.3.3 above.

4.4 Information Protection and Management

4.4.1 Sydney Opera House will ensure that no CCTV system will be used to invade the privacy of any individual (except for legal purposes or in accordance with this policy). CCTV cameras and monitoring systems will only be accessed and operated by appropriately

authorised officers for the purposes outlined in this policy and in accordance with EPRG standard operating procedures.

4.4.2 Recorded material and information from CCTV systems will be managed in accordance with the requirements *Privacy and Personal Information Act 1998* (NSW) and other relevant legislation and policies relating to the control of personal information.

4.4.3 Recorded material will be kept on the system for no longer than 30 days, after this period it will be written over. Where an incident occurs and it is captured on CCTV via the control room operator, recorded material will be retained and will be stored in a secure location that is only accessible by EPRG management.

4.4.4 Recorded material will only be retained for more than 30 days where it is required in relation to an investigation, incidents or legal proceedings, in which case retention and disposal requirements apply as specified in the NSW State Records Retention and Disposal Authorities.

4.5 System Use

4.5.1 All persons involved in the operation, use and maintenance of CCTV systems (operating staff) have a responsibility to ensure due care and diligence is exercised at all times to protect the integrity of systems and information, and to prevent improper disclosure of information.

4.5.2 Operating staff must undertake their duties in accordance with this policy and EPRG standard operating procedures.

4.5.3 Operating staff will undergo appropriate briefings and training on systems operation and security requirements prior to commencing operation of CCTV systems.

4.5.4 Control room operators have a responsibility to report to the Emergency Operations Duty Manager (EODM):

a) any safety related hazards or incidents that come to the notice of the officer while posted in the control room; and

b) any incidences involving a breach of the following:

- *Sydney Opera House Trust Act 1961*
- *Sydney Opera House By-law 2010*
- Emergency Management & Recovery Plan
- Sydney Opera House Code of Conduct
- any Sydney Opera House corporate policy or procedure.

4.5.5 Any misuse of CCTV systems, information and recorded material produced by the systems, or activity otherwise inconsistent with the conditions of this policy, is considered misconduct. Acts of misconduct will be subject to investigation and, depending on the outcomes of that investigation, may be subject to disciplinary action.

5 Monitoring and Review

5.1.1 CCTV systems, operation of those systems and compliance with this policy is subject to regular review and/or audit at the discretion of the Head of Security, Emergency Planning and Response, Executive or CEO.

5.1.2 This policy and associated procedures will be reviewed every two years or earlier if required in response to changes in legislation, industry standards or organisational arrangements.

6 Accountabilities

6.1.1 All operating staff are responsible for complying with this policy and any associated procedures at all times. Staff are also responsible for reporting any suspected breaches of this policy immediately to the Head of Security, Emergency Planning and Response.

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

- authorising access to CCTV systems and recorded material/information in accordance with this policy;
- monitoring use and performance of CCTV systems, including audit and risk assessment activities associated with CCTV systems and policy compliance; and
- the implementation, monitoring and review of this policy.

7 References

Workplace Surveillance Act 2005 (NSW)

Privacy and Personal Information Act 1998 (NSW)

Sydney Opera House Trust By-law 2010

Sydney Opera House *Code of Conduct*

Australian Security Industry Association *CCTV Code of Ethics*

APPROVED

Acting Chief Executive

Date: 31 July 2012