Closed Circuit Television (CCTV) Procedures

Section 1 - Purpose and Scope

(1) Safety and protection of people and assets can be facilitated by the use of closed circuit television (CCTV) systems. This procedure establishes the principles for installation and use of CCTV by Southern Cross University and operates subject to the Privacy Management Plan.

Section 2 - Scope

(2) This procedure applies to all SCU staff and students.

(3) This procedure does not apply to the recording, audio and screening of lectures made available by SCU.

Section 3 - Definitions

(4) Nil.

Section 4 - Procedures

(5) Southern Cross University seeks to protect people and assets in and around university property in the most effective manner possible including, where necessary, through the appropriate application of closed circuit television (CCTV) surveillance systems.

Scheme objectives, principles of operation and ownership

(6) The primary use of SCU CCTV is to discourage and/or detect unlawful behaviour in and around university property thereby enhancing the safety and security of all people and property. Other applications and benefits of SCU CCTV include traffic management and monitoring the utilisation of teaching and learning spaces so that the University's assets may be used in the most efficient and effective manner.

(7) Use of the SCU CCTV system is strictly restricted to activities which are:

a. reasonably necessary; and
b. for lawful purposes; and
c. directly related to SCU's functions or activities.

(8) Responsibility for the overall management of the SCU CCTV network, and authority to amend the network from time to time, rests with the Executive Director, Information and Physical Resources (ED, IPR).

Installation of Cameras and Method of Operation

(9) All security CCTV systems installed will comply with the following:

a. approval for the installation must be obtained from the Executive Director, Information and Physical Resources (ED, IPR) before the system is installed;
b. CCTV cameras must not be hidden;
c. all CCTV controls and recorders must be located in a secure area;
d. access to CCTV controllers and recorders will be limited only to authorised user(s);
e. all security CCTV equipment will be integrated into the university's wider electronic security network to enable effective monitoring by the university's security services;
f. cameras will not be located:
    i. so as to capture images from private property adjacent to the University; or
    ii. in any change room, toilet facility, shower or other bathing facility.

Signage

(10) Signage indicating a CCTV system is in operation will be displayed at common entry points to each SCU campus and other high volume traffic areas. Such signage will:

a. convey clearly that CCTV cameras are in place, preferably with the CCTV symbol; and
b. have been pre-approved by the Privacy Officer as compliant with the requirements of the Privacy and Personal Information Protection Act 1998.

(11) The signs must be located within normal eye range, be clearly visible, distinctive, and located in a position that is well lit.

Control Room Staffing and Operation

(12) The SCU CCTV control room will be staffed by either contracted security personnel or local SCU employees, who in both cases will be licensed security operators for the purposes of the Security Industry Act 1997.

(13) Training of CCTV related staff will be undertaken by the Security Supervisor (or their nominee) prior to the staff member commencing work with the CCTV system.

(14) Access to the control room will be restricted to persons having a lawful and legitimate need of access. With the exception of the licensed security operators employed to monitor the CCTV network and cleaning staff, any other person seeking access (except law enforcement officers - refer (18)) will require prior approval from the Executive Director, Information and Physical Resources (ED, IPR).

(15) Monitor operators must act with the utmost probity. The tracking or zooming in on any person must not be undertaken in a gratuitous or unreasonable manner. Camera operation is subject to audit and monitor operators may be called upon to explain their interest in a particular person.

Management of Data (including temporary access)

(16) CCTV recorded information must be:

a. used only for the purpose for which it was approved to be collected (unless expressly permitted for release by law);
b. stored securely;
c. accessed only by trained and qualified personnel;
d. restricted to access by user ID and password authentication (i.e. the use of generic user IDs, passwords or sharing of user IDs and passwords is not permitted);
e. clearly auditable for identification of individuals accessing the recorded information;

f. retained for a minimum period of 31 days, or, should the recorded material be required for investigation purposes, retained in accordance with legal requirements;
g. disposed of in a secure manner; and
h. protected from unauthorised access, use or disclosure.

Obtaining authorised access to data

(17) Requests to view recorded information will be assessed in accordance with the Privacy Management Plan.

Liaison with Law Enforcement

(18) Images may be released to the Police Service or other law enforcement agencies in compliance with relevant legislation. All requests made by the Police Service or other law enforcement agencies should be referred to the Security Supervisor who will advise the University Privacy Officer of the request and its result using the Law Enforcement Information Access Form.

Other third party access to data

(19) The University may release images and/or recordings to third parties, other than law enforcement, but will only do so if authorised or required to by the Privacy and Personal Information Protection Act 1998 (NSW).

Complaints

(20) Privacy related CCTV complaints will be managed in accordance with the Privacy Management Plan.

(21) CCTV complaints which are not related to privacy will be managed in accordance with the Complaints Policy - Students and Members of the Public.

Auditing

(22) An audit of CCTV incidents will be undertaken tri-annually to ensure all incidents are being logged and responded to in compliance with relevant legislation, standards and policies.

(23) A security audit will be undertaken tri-annually to ensure CCTV systems are adequately secured both physically and electronically.

Section 5 - Guidelines

(24) Nil.

Status and Details

Status	Historic
Effective Date	23rd June 2016
Review Date	23rd February 2019
Approval Authority	Vice Chancellor
Approval Date	23rd June 2016
Expiry Date	30th May 2017
Head of Work Unit	Danika Head Director, Property Services
Enquiries Contact	Governance Services