Closed Circuit Television (CCTV) Policy

Section 1 - Purpose and Scope

(1) The Closed Circuit Television (CCTV) Policy establishes the principles and operational procedures for the installation and use of CCTV by Southern Cross University.

(2) This policy applies to all SCU staff and students. It also applies to contractors, service providers, clients, customers and visitors.

(3) This policy does not apply to any recording or screening of lectures by SCU.

Section 2 - Definitions

(4) The following definitions apply to this Policy:

a. Closed Circuit Television (CCTV) means any combination of cameras, lenses, video/digital recorders and/or accessories installed for the purpose of monitoring and or recording visual activity.
b. Authorised User means a person authorised by the Vice President (Operations), or their delegate and contracted security personnel.

Section 3 - Policy Statement

(5) The University is committed to providing a safe and secure learning and working environment. Where necessary and appropriate the University will use CCTVs to protect people and assets in and around university property, while also respecting and protecting the individual's right to privacy. The use of CCTV is part of an integrated security approach that includes a number of strategies, including access controls, lighting, alarms and security staff.

Part B — Installation and Method of Operation

(6) Use of CCTVs is strictly restricted to activities which are:

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

Responsibility

(7) The Vice President (Operations) is responsible for the overall management of the University's CCTVs and has authority to amend or review the network from time to time.

Installation

(8) The following conditions apply to the installation of CCTVs:

a. The approval of the Vice President (Operations) must be obtained before the installation of a new camera;
b. CCTV cameras can only be installed by persons who are appropriately licensed under any relevant legislation.
c. CCTV cameras must not be hidden and must 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.
d. All CCTV controls, monitors and recorders must be located in a secure area.
e. Access to CCTV cameras will be limited only to Authorised User(s).
f. All CCTV equipment will be integrated into the University's wider electronic security network to enable effective monitoring by the University's security services.
g. When a CCTV camera is scheduled for replacement, the Manager, Facilities Management and Services will make a recommendation to the Vice President (Operations) about whether the camera should be replaced.

Signage

(9) 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.

(10) The signage will:

a. be located within normal eye range, be clearly visible, distinctive, and located in a position that is well lit;
b. convey clearly that CCTV cameras are in place, preferably with the CCTV symbol; and
c. have been pre-approved by the Privacy Officer as compliant with the requirements of the Privacy and Personal Information Protection Act 1998.

Monitoring

(11) The SCU CCTV control room will be staffed by Authorised Users.

(12) The Security Supervisor, or their nominee, will ensure Authorised Users are aware of the University's policy and procedure before commencing work with the CCTV system.

(13) Access to the control room will be restricted to persons having a lawful and legitimate need of access. Individuals require prior approval of the Vice President (Operations) is required to gain access to the control room, with the exception of:

a. Authorized Users;
b. cleaning staff; and
c. law enforcement officers (refer clause(18)).

(14) Authorized Users 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.

(15) CCTV recorded information must be:

a. used only for the purpose for which it was approved to be collected (or as otherwise authorised or required by law);
b. stored securely on a secure SCU computer server;
c. accessed only by Authorized Users;
d. restricted 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 and allow for the identification of individuals accessing the recorded information;
f. retained for a minimum of 45 days;
g. disposed of in a secure manner; and
h. protected from unauthorised access, use or disclosure.

(16) The Manager, Facilities Management Services will be responsible for monitoring compliance with the CCTV Policy and will report annually to the Vice President (Operations) regarding the use and management of the CCTV system.

(17) The Director, Technology Services, in consultation with the Manager, Facilities Management Services, will ensure an audit is undertaken annually as to the physical and electronic security of the CCTV system.

Obtaining authorised access to data

(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.

(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).All other requests to view recorded information will be assessed in accordance with that Act and the Privacy Management Plan.

Complaints

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

(21) All other complaints will be managed in accordance with the Complaints Policy - Students and Members of the Public.

Section 4 - Procedures

Approval and Authority

(22) A weekly report on the monitoring of CCTV will be provided to the Manager, Facilities Management Services by the Head of Security.

Monitoring (Operation)

(23) The CCTV system will generate a live feed which will be visible in the control room. The monitoring room will be used only for the purpose of monitoring the CCTV system and access is restricted as per clause (13). Access to the room will be with a personally coded swipe card.

(24) Recordings and data produced by the CCTV system will be retained for a period of no more than 45 days. The Manager, Facilities Management Services may determine to retain recordings, and data produced by the CCTV system for more than 45 days where it is allowable to do so under the CCTV Policy and the Privacy Management Plan. Other than that, CCTV footage is automatically overwritten after 45 days.

Training

(25) All security officers at the University will receive training with regards to the capabilities of the CCTV system installed. This training will include:

a. camera locations;
b. the responsibilities of Authorized Users when viewing recordings and making recommendations regarding further review;
c. the CCTV Policy;
d. the Privacy Management Plan; and
e. all relevant legislation.

Status and Details

Status	Historic
Effective Date	31st May 2017
Review Date	31st January 2020
Approval Authority	Vice Chancellor
Approval Date	24th May 2017
Expiry Date	17th September 2019
Head of Work Unit	Danika Head Director, Property Services
Enquiries Contact	Office of the Vice President (Operations)