



POLICY FOR CLOSED CIRCUIT TELEVISION SYSTEMS (CCTV)

OPERATED BY THE UNIVERSITY OF WESTERN AUSTRALIA

TABLE OF CONTENTS

1.....	<u>INTRODUCTION</u>
2.....	<u>STATEMENT OF PURPOSE</u>
3.....	<u>SYSTEM DETAILS</u>
4.....	<u>DATA PROTECTION - PRIVACY</u>
5.....	<u>MANAGEMENT OF THE SYSTEM</u>
6.....	<u>HALLS OF RESIDENCE AND COLLEGES</u>
7.....	<u>ACCOUNTABILITY</u>
8....	<u>PUBLIC INFORMATION</u>
9...	<u>ASSESSMENT OF THE SYSTEM AND POLICY</u>
10...	<u>OPERATING STAFF</u>
11...	<u>COMPLAINTS</u>
12...	<u>BREACHES OF THE POLICY INCLUDING THOSE OF SECURITY</u>
13...	<u>CONTROL AND OPERATION OF THE CAMERAS</u>
14...	<u>ACCESS TO AND SECURITY OF MONITORS AND SECURITY CONTROL ROOM</u>
15...	<u>RECORDED MATERIAL</u>
16...	<u>DEALING WITH INCIDENTS</u>

DEFINITIONS

- *Agent*: An officer authorised by the Director Facilities Management to act on his behalf under this Policy. Normally the Manager, Security and Parking unless otherwise stated.
- *Contractor*: Contractor employed by the University to install/maintain the CCTV system.
- *Control Room*: The restricted access facility managed by the Manager, Security and Parking.
- *Logbook*: The log used by UWA Security to record incidents occurring during a Security shift.
- *Authorities*: WA Police, Australian Federal Police, Emergency Services and other agencies.
- *Register*: Transmittal register used to record the transmission, archiving or disposal of tape media containing visual images recorded using the University CCTV system.
- *Security Officer*: UWA Security Officer.
- *Staff Member*: UWA Staff member

1. INTRODUCTION

1.1. The University of Western Australia is highly regarded for its reputation as an open safe accessible campus. This policy document has been developed to comply with legislative requirements and standards. The policy will be applied to the management of closed circuit television systems (CCTV) established on the UWA campus and managed by Facilities Management Division (UWA Security) from the Central Control Room. Other CCTV systems installed by a School, Faculty, Division, Business Unit, Hall of Residence, College or Tenant of the University of Western Australia are expected to follow the same policy and procedures.

1.2. The CCTV system will be managed in accordance with all relevant legislation, standards and University policies. Monitoring of cameras, and any replay of recorded footage, is controlled by the Workplace Video Surveillance Act 1998.

1.4. The Director, Facilities Management is responsible for managing adherence with the conditions laid down in the policy. Any changes or extensions to the policy or system will only take place after consultation with relevant University management. The Director, Facilities Management may authorise an agent to approve minor changes to the system and to this policy, where appropriate. Minor changes are those that do not have a significant impact on the intent of the policy or the procedures established to monitor adherence with its provisions.

2. STATEMENT OF PURPOSE

2.1. The University CCTV system is primarily intended to provide an increased level of service, safety and security in the University environment. The use of CCTV is part of an integrated security approach that includes a number of strategies, including a physical security presence, access control and alarms.

CCTV systems on campus may also be used for training purposes, or managing access control and will not be used to invade the privacy of any individual. For the purpose of this policy, the University environment includes all University land and buildings, including those areas occupied by Colleges and commercial businesses.

2.2. The system will only be used for the following purposes:

- a. To limit, deter and detect crime and criminal damage;
- b. To identify, apprehend and assist in prosecuting offenders;
- c. To improve communications and the operational response of staff ;
- d. To assist emergency services ;
- e. To assist in access control, particularly vehicle access to the inner campus ;
- f. To assist staff in operating audio visual equipment.

2.3. Any misuse of this system or materials produced as a consequence which is frivolous, or for private purposes, or is otherwise inconsistent with the objectives and procedures outlined within this policy may attract penalties up to and including those attached to instances of serious misconduct.

2.4. As community confidence in the system is essential, all cameras will be operational. An appropriate maintenance program will be established.

3. SYSTEM DETAILS

3.1. The CCTV System consists of a number of overt colour CCTV cameras situated on University property, which continuously record activities in that area. In some circumstances these systems are linked to the Facilities Management Virtual Local Area Network (VLAN) or are accessible to the University. Security Systems linked to the Facilities Management VLAN must comply with the *Specification for the University of Western Australia Integrated Security Systems Works Standards* (Available through Facilities Management Planning and Design). The security control room is also equipped with a licensed radio system linking security patrols and the control room.

4. DATA PROTECTION - PRIVACY

4.1. All data collected using this system, including images, will be managed in accordance with the relevant Federal and State laws and University policy relating to the control of private information.

4.2. All persons involved in the operation of the system are obliged to exercise the upmost care to prevent improper disclosure of material.

5. MANAGEMENT OF THE SYSTEM

5.1. Facilities Managements Division (UWA Security and Parking) is responsible for managing compliance with this Policy, including compliance by staff and contractors employed to work on the system or in the Control Room.

5.2. The Manager, Security and Parking, shall be responsible for the day-to-day management of the system and associated processes. In particular, the Manager, Security and Parking will be responsible for external agency liaison, compliance with the Policy and Operational Manual by staff, contractors or any other authorised person, staff training, the preparation of reports and the evaluation of the system performance.

5.3. The Manager, Security and Parking will be responsible for managing the Security Control Room, ensuring that only authorised personnel are given access.

5.4. Schools, Faculties, Divisions, Business Units or Tenants having CCTV are to ensure appropriate restricted access only is granted to the system.

5.5. Prior to any extension of the system being approved the following actions will be completed:

- a. The Facilities Managements Division will conduct a needs assessment and prioritisation of risk management objectives.
- b. Consultation shall be undertaken between the Division and the local areas (and any other parties affected by the extension) prior to an application being made to the Facility Development Committee. Executive approval of any new or extension to the system will be required.

5.6. Compliance by University staff (specifically Security and Parking officers) and contract staff will be subject to audit. These audits will be conducted as required and at least once per year. The Director, Facilities Management will appoint an independent staff member to undertake the audit and provide a written report for the University Executive.

6. HALLS OF RESIDENCE AND COLLEGES

6.1. It is recognised that the Residential Colleges are entities in their own right on University lands. Residential areas camera locations and key objectives should be the subject of consultation with resident groups, including defining areas that will be considered private. The Colleges have an obligation to ensure that appropriate operational procedures are adopted that impose restraints upon the use of cameras in connection with private residences.

7. ACCOUNTABILITY

7.1. The University acknowledges the importance of accountability in the management of the system. With that in mind, the following steps will be taken to ensure the campus community is informed:

- a. Copies of this policy will be available to the public via the University web page.
- b. An annual report to the University Executive on the operation of the system will be prepared by the Director, Facilities Management or agent. This report will provide information on any extensions to the system (ie, additional cameras) and changes to the policy.

8. PUBLIC INFORMATION

8.1. Cameras will not be hidden and will be placed in public view wherever possible.

8.2. Signs that CCTV cameras are operating will be displayed at key positions and in proximity to the area under surveillance to allow people to be made aware that highly visible CCTV systems operate within the University.

8.3. The policy will be available on the University web page.

9. ASSESSMENT OF THE SYSTEM AND POLICY

9.1. The Facilities Managements Division is responsible for ensuring that the System is evaluated annually by the Director or his authorised agent.

9.2. Evaluation will be conducted according to the following criteria:

- a. Impact on crime/damage/public order.
- b. Operation of the policy.
- c. Impact on the Universities reputation.

9.3. Ongoing monitoring of the system will be conducted by the Manager, Security and Parking who will also take all reasonable measures to ensure that all relevant parties are complying with the provisions of this policy.

10. OPERATING STAFF

10.1. University staff and contractors employed to work on the system must be fully cognisant of their responsibilities under this policy.

11. COMPLAINTS

11.1. Complaints regarding the CCTV system and its operation must be made in writing to the Director, Facilities Management. Where appropriate, the Director will appoint an independent person to investigate the complaint and provide a written report within an agreed period of time not to exceed eight weeks. The report will be presented to the Director, Facilities Management, who will take action as appropriate within University guidelines and advise the complainant. Where the complainant is not satisfied with the resolution, the complaint can be directed to the Vice-Chancellor for investigation and action as appropriate. For this policy, the definition of an independent person is one who does not directly work in areas responsible for the management or maintenance of the CCTV system.

12. BREACHES OF THE POLICY INCLUDING THOSE OF SECURITY

12.1. Breaches of the policy and of security must be subject to proper investigation by, in the first instance, the person appointed by the Director Facilities Management to conduct an investigation. This person shall be responsible for making recommendations to the Director, Facilities Management to remedy any breach.

12.2. The University reserves the right to apply disciplinary measures for breaches, up to and including referring the breach to appropriate relevant authorities.

13. CONTROL AND OPERATION OF THE CAMERAS

13.1. Control Room equipment and the remote control of cameras will only be operated by authorised persons acting with the utmost probity.

13.2. Operational procedures shall be adopted to ensure necessary restraints upon the use of cameras in relation to private premises.

13.3. System Operators will be subject to supervisory procedures and routine audit to ensure compliance with this aspect of the policy.

13.4. The Manager, Security and Parking will be responsible for the control, storage and approved use of recorded material.

14. ACCESS TO AND SECURITY OF MONITORS AND SECURITY CONTROL ROOM

14.1. Access to and operation of equipment or viewing of images should be limited to authorised staff.

14.2. Access to or the demonstration of monitors will not be permitted except for lawful and proper reasons.

15. RECORDED MATERIAL

15.1. Recorded material will be used only for lawful purposes defined in this policy. Access to recorded material will only take place as defined in the policy. Recorded material will not be sold or used for commercial purposes.

15.2. Still photographs from incidents will only be taken at the request of the Director, Facilities Management, Manager, Security and Parking or the appropriate authorities. A written record of the request including details of the requesting officer, time and date of the request and the reasons will be made. This record will be held by the Manager, Security and Parking.

16. DEALING WITH INCIDENTS

16.1. Consistent with standard operating procedures control room operators are authorised to report relevant matters to authorities as appropriate. A record of any reports will be made at the time and will include details of the incident, date and time of the report and details of the officer taking the report. Where appropriate, the control room operator may elect to have a University security patrol attend the incident before making a formal report to the authorities or emergency services.

16.2. All incidents requiring attendance by the authorities will be reported to the Manager, Security and Parking.

NOTES

For Manager, Security and Parking read also Security Superintendent, or any other officer so appointed by The Director, Facilities Management.

REFERENCES

- AS 4806.1-2006 Closed Circuit Television (CCTV) Part 1: Management and Operation.
- Surveillance Devices Act 1998 (WA)
- Privacy Act 1998 (Commonwealth).
- Works Specification for the University of Western Australia Integrated Security Systems Works Standards.

Date created:	Jan 2007	Approved by:	Executive Director, Finance and Resources
Previous	NA	Responsible:	Director, Facilities Management

edits:			
Date for review:	Dec 2007	File ref:	F 16114
Previous titles:	N/A		