Controlled Areas Security and Access Policy

Section 1 - Purpose

(1) The Charles Sturt University (the University) has the right to regulate access to University premises and to control the entry of vehicles and their operations within premises.

(2) This Policy aims to provide a clear and unambiguous document from which staff and Campus Security Officers can develop procedures that will assist them to carry out their duties effectively and efficiently; particularly in relation to managing persons who are about to commit, are committing or have committed an offence or breach of the law or a breach of University Rules or who are engaging, or about to engage, in disorderly conduct.

(3) The objectives are to:

a. provide a safe and secure physical environment, as far as practicable, for staff, students, contractors and visitors and to maximise the protection of University property;

b. ensure students, staff and visitors enjoy the social and academic benefits of the University;

c. minimise, as far as practicable, the number, range and impact of incidents on University teaching and research activities, buildings and infrastructure and people;

d. implement security services and systems that reflect organisational policy and maintain a trained and flexible security workforce that can be adapted to meet the University's changing needs; and

e. empower staff to appropriately respond to incidents and emergencies in accordance with documented operating procedures and manuals which are informed by this Policy.

(4) This Policy is subject to relevant state, territory and Commonwealth law and the University's Rules.

Scope

(5) This Policy applies to all staff, students, third party contractors who provide security services to the Charles Sturt University and visitors to University premises within Australia.

References

(6) This Policy aims to be consistent with, and is to be read in conjunction with the following:

a. Charles Sturt University Act 1989 (NSW);

b. Inclosed Lands Protection Act 1901 (NSW) and Inclosed Lands Protection Regulation 2008 (NSW); and

c. Security Industry Act 1997 (NSW) and Security Industry Regulation 2007 (NSW).

(7) Standard operating procedures associated with this Policy will be incorporated into instructions and training materials which will be made available to authorised officers. All authorised officers are to be fully conversant with these procedures prior to commencing duties at the University and throughout their employment.

Section 2 - Glossary

(8) In this Policy, unless the contrary intention appears:

a. Access Control - means any method for controlling access to controlled areas including electronic code-pads, card readers and other RFID (Radio Frequency Identification) devices, remote arming stations, passive infra-red detectors, duress buttons, reed switches, mechanical barriers, locks, and the use of Charles Sturt University Identification Cards, signs, border definitions and instructions used to define semi-public and private spaces which certain people may or may not enter.

b. Access Control Device - means any electronic access control device or token such as a magnetic strip card, proximity card or key-ring fob and other RFID devices which can be used to activate a locked or electrically controlled door, turnstile, boom-gate or similar barrier when programmed to do so. For the purposes of this Policy the word 'card' may include a Charles Sturt University identification card and may be extended to include codes or personal identification numbers (PIN) used for access purposes.

c. Alarm System - means any electronic intruder detection, hold-up or duress alarm system installed for the purpose of detecting or signalling security related incidents.

d. Authorised CCTV operator - means a person authorised by the Director, Operational Services, Division of Facilities Management(or delegate) who has successfully completed Charles Sturt University security CCTV training and is conversant with this Policy and applicable legislation.

e. Authorised officer - means:
    i. the Vice-Chancellor;
    ii. the Chief Financial Officer;
    iii. Director, Operational Services, Division of Facilities Management;
    iv. Campus Services Manager, Division of Facilities Management;
    v. Client Service Co-ordinators, Division of Facilities Management;
    vi. Director, Residence Life, Division of Finance;
    vii. Campus Security Officers, Division of Facilities Management;
    viii. senior members of staff appointed by the Vice-Chancellor for the purpose of this Policy; and
    ix. any person appointed as an authorised officer in accordance with Part A of this Policy.

f. Campus Security Officer - means any person engaged by the University (either as staff or third party contractors) to provide security services or traffic control functions in relation to University premises.

g. Closed Circuit Television System (or CCTV) - means any combination of cameras, lenses, video/digital recorders and/or accessories installed for the purpose of monitoring and/or recording visual activity that complies with the DFM CCTV design and installation specification.

h. Controlled Area - means any area or space on University premises to which general or public access is not available at that time. This may be characterised by signs, locked doors, fences, boom-gates, sentinel tape, or be defined by the instruction of a Campus Security Officer or designated member of staff.

i. Critical Assets - means any Charles Sturt University equipment, infrastructure, documents or intellectual property, the loss of which would seriously impact on the activities of the University.

j. University - means Charles Sturt University.

k. Charles Sturt University Identification Card - means an official photographic identity card issued by Student Central, which may, or may not, additionally function as an access control device.

l. University Rules - means the Charles Sturt University Act 1989 (NSW), Charles Sturt University By-Laws, rules, regulations, policies, guidelines, and procedures, applying to students, staff, contractors and/or visitors.

m. DFM - means Division of Facilities Management.

n. Enterprise Agreement - means the Charles Sturt University Enterprise Agreement 2010-2012, or other

applicable industrial instrument.

o. Faculty/Division/Centre Access Coordinator - means a Faculty/Division/Centre staff member authorised by the relevant Executive Dean, Executive Director or Centre Director to grant, deny or revoke access privileges to Controlled Areas for which the Faculty, Division or Centre is directly responsible.

p. Monitored Alarm System means an alarm system which is connected via LAN, WAN, PSTN, cable, radio transceiver or other means to a central monitoring station, or University security control room, or automatic SMS, voice message or visual alarm forwarding system, which will communicate system alerts and facilitate appropriate responses to alarms.

q. Security Incident - means any situation arising that may compromise the security of people, assets or property on University premises including, for example, acts of violence, theft or damage, suspicious or threatening behaviour, activation of any alarm, any instance of unauthorised access, disorderly or unlawful conduct and any emergency situation such as fire, flood or accident.

r. Security - means the security office of each campus and any campus security manager or officer.

s. Security Licence - means an appropriate licence granted under the [Security Industry Act 1997](#) NSW or the Security Industry Act 2003 ACT or equivalent legislation in any other relevant jurisdiction.

t. Security Management means DFM's Campus Services Manager, the Manager, Operations and Maintenance and the Director, Operational Services, Division of Facilities Management who are employed by the University to manage security operations and Security.

u. Staff - means all continuing, fixed term, casual or contract employees of the University.

v. Student - means a person who has been accepted for admission to or enrolled in any course or program offered at, or in conjunction with Charles Sturt University, or whose body of work, completed whilst so enrolled (e.g. a research thesis), is still under examination.

w. Supervising Staff Member - means every member of staff responsible for the provision of teaching or supervision of students, staff, contractors or visitors to the University in connection with a teaching or administrative activity (such as a lecture, tutorial or practical demonstration).

x. University premises - includes any land which is owned, controlled, managed or occupied by the University together with any building, construction or facility of any kind, whether permanent or temporary, on that land and also includes any other building, construction or facility which is under the control or management of, or which is occupied by the University. This excludes any building sites under the control of a head contractor.

y. Visitor - is any person who is not a student or member of staff but who accesses University premises.

Section 3 - Policy

Part A - Appointment of Authorised Officers

(9) The Vice-Chancellor, or nominated delegates, may appoint, in writing, any person they are satisfied has the necessary training, knowledge and experience to act on their behalf as an authorised officer to exercise the powers set out in Part B below.

(10) Authorised officers may include staff or third party contractors engaged to perform security duties under a contract with the University.

(11) Authorised officers must have their Charles Sturt University identification card or security licence prominently displayed at all times or be able to produce this on demand.

Part B - Powers of Authorised Officers

Regulate the Access and Behaviour of Persons on University Premises

(12) An authorised officer is entitled to:

a. make enquiries and take reasonable action, in compliance with this Policy and related documents (including clauses 26 and 27), to regulate the access and behaviour of staff, students, visitors and members of the public whilst they are on University premises in order to maintain a safe and secure environment;

b. request any person on University premises to produce proof of identity; and

c. make reasonable and necessary enquiries to validate that person's status if they are unable to produce their Charles Sturt University identification card or otherwise justify their right to be on University premises.

Request to Leave University Premises

(13) An authorised officer may, at any time, request a person to leave University premises if:

a. they are unable to produce appropriate identification or justification for being on University premises;

b. the authorised officer has reasonable grounds to believe that the person has committed, is committing or is about to commit a criminal act, or breach University Rules;

c. the person is involved in disorderly conduct (see clauses 26 and 27); or

d. the person is acting in a way that may threaten public order, damage property or otherwise pose a threat to the safety and wellbeing of persons on University premises.

(14) Authorised officers should call the police for assistance where any person refuses to comply with a request to leave the University premises.

Traffic and Parking

(15) Authorised officers are empowered, in accordance with this Policy, to administer and control vehicle access to University premises and the traffic and parking provisions therein.

Supervising Staff Members

(16) Every supervising staff member is empowered to request a student involved in disorderly conduct (as described in clauses 26 and 27) during a teaching activity (such as lecture, tutorial or practical demonstration) that impedes the normal functioning of that activity to leave the activity for its duration, provided that:

a. the supervising staff member has in the first instance requested the student to discontinue the disorderly conduct; and

b. the supervising staff member reports each exercise of this power to the Executive Dean of the relevant Faculty, the Campus Services Manager, Division of Facilities Management and the Academic Registrar (for consideration of the conduct as possible general misconduct by a student).

(17) Note: If a student refuses to comply with a request by a supervising staff member to leave a teaching activity, staff are advised to contact Security for further assistance.

Part C - Police, Emergencies and Disorderly Conduct

Police Powers

(18) Nothing in this Policy limits the right of any State, Territory or Federal Police Officer to enter University premises and/or to take action consistent with their relevant authorities and powers, either in an emergency situation or as part of their general services to the public.

Special Police Operations

(19) Police may, from time to time, conduct specific operations on University premises.

Communication

(20) If any member of Security calls the police to University premises, they must immediately inform a member of Security management. Depending upon the nature of the event, the Campus Services Manager, Division of Facilities Management or Head of Campus may inform the Chief Financial Officer.

Emergencies

(21) If any staff or student calls the police to University premises, then they must inform a member of Security as soon as possible and advise them of the nature of the emergency so Security can co-ordinate and expedite police attendance at the emergency site.

(22) A head contractor in control of a building site is to have emergency arrangements in place. However, the contractor may require assistance from an authorised officer from time to time to coordinate emergency response, site access etc.

Security Incidents

(23) All Security Incidents which occur on University premises are to be reported to Security. Security is responsible for ensuring police are notified of all minor incidents on University premises where appropriate, including those relating to the loss or damage of University property.

(24) It is the responsibility of any individual who has suffered loss of or damage to personal property to notify police and Security. Once notified, Security shall attend the site and complete a University Security Incident Report.

Political Statements or Protests

(25) Where any member of staff or Security becomes aware that a political protest or demonstration is planned or taking place on University premises, they must immediately notify a member of Security Management.

Disorderly Conduct

(26) Disorderly conduct is recognised as general misconduct. For details of categories of general misconduct refer to the Enterprise Agreement, Student General Misconduct Rule and the Code of Conduct for Staff.

(27) In the interpretation of this Policy, the following forms of conduct will be considered 'disorderly conduct' and may lead to action being taken by authorised officers to maintain good order and orderly conduct on University premises:

  a. failure to comply with University Rules;
  b. conduct which impairs the reasonable freedom of other persons to pursue their studies, research, duties or lawful activities in the University or to participate in the life of the University;
  c. conduct that threatens the health, safety or welfare of staff, students or visitors of the University;
  d. wilful failure to obey any reasonable direction of authorised officers in relation to University premises, access and order;
  e. failure to furnish or provide appropriate identification on request by an authorised officer;
  f. wilfully entering any place on University premises which the person is forbidden to enter under University Rules or by an authorised officer;
  g. wilfully littering the University premises or damaging, defacing, or wrongfully dealing with any University property or any other property on University premises; and

h. any other unreasonable conduct disrupting the normal activities of the University.

Complaints of Alleged Disorderly Conduct - Risk to Safety

(28) If an incident occurs which is a threat or risk to personal safety, or which requires immediate intervention, individuals are advised to contact Security and/or the Police immediately.

Complaints about Disorderly Conduct by Students

(29) Complaints reported to Security alleging disorderly conduct by students of the University should be reported to the Head of Campus as soon as practicable after the alleged misconduct has occurred.

Complaints about Disorderly Conduct by Staff

(30) Complaints reported to Security alleging disorderly conduct by staff should be reported to the Head of Campus as soon as practicable after the alleged misconduct has occurred.

Complaints about Disorderly Conduct by Other Members of the University Community

(31) Complaints alleging disorderly conduct against non-student and non-staff members of the University community should be brought to the Head of Campus by authorised officers, a student or a staff member as soon as practicable after the alleged misconduct has occurred.

Part D - Role of Security

(32) The role of Security is to provide staff and students with a safe and secure environment which facilitates and promotes learning and research.

(33) When exercising their responsibilities under the relevant law, University Rules and conditions of appointment, all Security staff must fulfil their duties in a fair and equitable manner without damage to the University's reputation or unfairly impinging on the rights of the individual.

(34) The duties of Security include taking reasonable action to assist with:

a. the prevention and investigation of crimes against the person on University premises e.g. assaults, offensive behaviour, indecent exposure, trespass etc. and reporting suspected crimes to, the Campus Manager and the police or other relevant external authorities;

b. the prevention and investigation of property crimes on University premises e.g. wilful damage, theft, burglary etc. and reporting suspected crimes to the Campus Manager and the police or other relevant external authorities;

c. the maintenance of public order on University premises;

d. the management of emergencies e.g. fires, chemical spills, injury etc., including reporting emergencies to the Campus Manager police, fire, ambulance or other relevant external authorities;

e. the provision of a client centred service that extends beyond the boundaries of a traditional patrol role. Security staff are often the first or only available contact the public has with the University; and

f. otherwise ensuring staff, students and visitors comply with the law and University Rules whilst on University premises.

Part E - Access to University Premises

Persons Eligible for Entry

(35) Staff, students and other persons with a valid reason to access University premises may enter University premises, provided that:

    a. entry has not been prohibited by any authorised officer; and

    b. they comply with any conditions which may be applicable to their access to the University premises.

(36) Please refer to the Controlled Areas Security and Access Procedure for information about the categories and level of access of eligible persons.

University Identification Cards

(37) All members of staff (including contract and casual staff) and students of the University are issued with University identification cards which must be:

    a. carried during attendance at University premises; and

    b. shown in response to any reasonable request from any authorised officer or from any other member of staff who might require such identification in the course of their duties.

Access to Controlled Areas

(38) DFM is responsible for managing the University's access control systems which provide access to controlled areas.

Access Control Devices

(39) The selection, installation, maintenance and operation of all electronic access control devices and equipment at University premises must be made in consultation with and prior approval of DFM.

(40) Access control devices are issued by the University to allow students, staff and contractors access to controlled areas of the University.

(41) Access control devices must be used in accordance with any accompanying instructions.

(42) All persons to whom an access control device has been issued must only use the access control device to enter areas of University premises for which they are currently authorised.

(43) Access control devices must be used only by the person to whom they have been issued. They must not be lent, given to or used by any other person to enter a controlled area for which they have no authorised right of entry.

(44) Anyone possessing or using an access control device to enter University premises without authorisation will be subject to disciplinary action from the University, or criminal charges where appropriate.

(45) To ensure compliance with applicable fire and building safety codes, non-University approved access control equipment must not be used.

(46) Fabrication of any access control devices must only be performed or facilitated by authorised staff. Any unauthorised fabrication, duplication, issuing, possession, or use of access control devices is strictly prohibited.

(47) Access control devices remain the property of the University and must be returned on demand at any time.

Keys and Locks

(48) An important outcome of this Policy is to ensure uniformity and compatibility of keys at all University premises and for the maintenance of central key records.

(49) This Policy applies to all facility keys, including keys for all doors and all gates, as well as for cabinets or safes which were originally keyed through DFM, on all University premises.

(50) DFM is responsible for promoting the uniformity and compatibility of keys used at University premises, and for the maintenance of central key records.

(51) Any key equipment of the University (including key, lock and door furniture) intended to be installed or used at any University premises must be of a type approved and specified for the particular application by DFM (excluding a building site managed by a head contractor).

(52) To ensure compliance with applicable fire and building safety codes, non-University approved mechanical keys or locks must not be used.

(53) Fabrication (including duplication) of University keys must only be performed or facilitated by authorised staff within DFM. Locks must not be altered, replaced or refitted without prior permission of DFM. Any unauthorised fabrication, duplication, issuing, possession, or use of University keys is strictly prohibited.

(54) University keys remain the property of the University and must be returned on demand at any time.

(55) Access to University premises is the responsibility of and controlled by DFM. A University Faculty/Division/Centre which has been assigned space within a building or area of enclosed property shall be responsible for the management and control of keys to those areas. A Faculty/Division/Centre assigned tenancy to any space is responsible for approving internal access within that space as directed by the Faculty/Division/Centre's's access coordinator.

Part F - CCTV Usage

(56) The primary use of CCTV is to discourage unlawful behaviour and to assist in the successful prosecution of individuals involved in unlawful behaviour in and around University property, thereby enhancing the safety and security of people and property. Other applications and benefits of CCTV include traffic management and assisting some access control activities.

(57) Only security CCTV equipment, applications and monitoring specifications which are included in the University's CCTV technical guidelines (approved by DFM) shall be applied to University premises. Appropriate standard operating procedures shall be applied to all security CCTV applications to ensure effective and ethical management of equipment and that the recorded information is appropriately maintained by authorised CCTV operators. All security CCTV systems installed will comply with the following:

   a. all CCTV controls and recorders must be located in a secure area;
   b. appropriate signage must be installed;
   c. access to CCTV controllers and recorders shall be limited to authorised CCTV operators only;
   d. all security CCTV equipment shall be integrated into the University's wider electronic security and access control system to enable effective monitoring by Security; and
   e. all CCTV equipment is to be used in accordance with any relevant legislation or applicable codes of practice.

Part G - Electronic Security Alarms

(58) The primary use of alarm systems is to protect persons and property by providing a means to deter, deny and/or detect unlawful behaviour.

(59) University property containing critical assets, highly confidential or sensitive information or for staff performing tasks which may be accompanied with a higher than usual security related risk should, as part of a total security solution, be considered for protection by a suitable monitored alarm system.

(60) Everyone within the University community has a responsibility to consider their own environmental security issues and are encouraged to seek professional advice from DFM regarding the most appropriate security solutions. This may include alarm systems such as personal duress alarms.

(61) DFM has responsibility for selection, installation and maintenance of all alarm systems in university premises.

Part H - Security Master Licence

(62) The Security Industry Act 1997 requires the University to maintain a current 'Security Master Licence' if it employs staff as Campus Security Officers to carry out 'security activities' as defined under the Act. The responsible officer for the University's Security Master Licence shall be the only person who can authorise the employment of staff as Campus Security Officers.

(63) Under no circumstances shall any persons be employed or engaged by the University as a member of Security without the express written consent of the Security Master Licence holder.

Section 4 - Procedures

(64) Nil.

Section 5 - Guidelines

(65) Nil.

Status and Details

Status	Historic
Effective Date	22nd May 2014
Review Date	15th February 2018
Approval Authority	Deputy Vice-Chancellor (Administration)
Approval Date	21st May 2014
Expiry Date	19th July 2018
Unit Head	Stephen Butt Executive Director, Division of Facilities Management +61 2 69332851
Author	Wayne Millar Director, Operational Services +61 2 69334220
Enquiries Contact	Wayne Millar Director, Operational Services +61 2 69334220