Security and Access to University Premises Policy

Section 1 - Purpose

(1) This Policy outlines security and access measures for Charles Sturt University's controlled areas and provides guidance to staff with administration responsibilities regarding security and access to Charles Sturt University (the University) premises. To ensure the security and safety of all staff, students and visitors and protection of University property; the University has the right to regulate access to University premises, including the control of vehicles and their operations.

(2) The objectives of this Policy are to:

a. provide a safe and secure physical environment, as far as practicable, for staff, students, and visitors (including contractors);
b. protect university property;
c. ensure students, staff and visitors enjoy the social and academic benefits of the University;
d. minimise the number, range and impact of incidents on teaching and research activities, infrastructure and people; 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.

Scope

(3) This Policy applies to all staff, students of the University and to visitors to University premises including contractors and members of the public.

(4) This Policy is subject to relevant State, Territory and Commonwealth law and University rules as identified under References.

References

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

a. Charles Sturt University By-law 2005;
b. Charles Sturt University Act 1989 No 76;
c. Inclosed Lands Protection Act 1901 No 33;
d. Inclosed Lands Protection Regulation 2018;
e. Security Industry Act 1997 No 157;
f. Security Industry Regulation 2016;
g. Animals on University Premises Policy;
h. Code of Conduct;
i. Critical Incident Response Group Procedure;
j. Emergency Management Policy;
k. Student Misconduct Rule 2020;

l. Space Management Policy;
m. relevant standard operating procedures associated with this Policy which are incorporated into instructions and training materials made available to Authorised Access Officers;
n. Charles Sturt University Enterprise Agreement; and
o. Work Health and Safety Act 2011 No 10 (NSW)

Section 2 - Glossary

(6) For the purpose of this Policy unless otherwise indicated:

a. Access Control Devices - means any method for controlling access used to define and control spaces (controlled areas) to which access restrictions apply including:
    i. electronic code-pads;
    ii. card readers and other Radio Frequency Identification Devices (RFID);
    iii. proximity cards or key-ring fob devices
    iv. remote arming stations;
    v. passive infra-red detectors;
    vi. duress buttons;
    vii. reed switches;
    viii. mechanical barriers;
    ix. locks and keys;
    x. university identification cards;
    xi. signs; and
    xii. border definitions and instructions.
b. Access Coordinator - means persons assigned responsibility for the management of access control devices by the relevant Authorised Access Officer.
c. Alarm System - means any electronic intruder detection, hold-up or duress alarm system installed for the purpose of detecting or signaling security related incidents.
d. Authorised Access Officer - means a staff member or University security contractor appointed in writing by the Vice-Chancellor or nominated delegates to exercise the responsibilities set out in Part C - Responsibilities:
    i. the Vice-Chancellor;
    ii. the Chief Financial Officer;
    iii. Executive Director, Division of Facilities Management;
    iv. Director, Operational Services, Division of Facilities Management;
    v. Manager, Operational Services, Division of Facilities Management;
    vi. Manager, Campus Services, Division of Facilities Management;
    vii. Manager, Client Services and Computing, Division of Facilities Management;
    viii. Director, Residence Life, Division of Finance;
    ix. Head of Campus;
    x. Campus Security Officer;
    xi. senior members of staff appointed by the Vice-Chancellor for the purpose of this Policy; and
    xii. any person appointed as an Authorised Access Officer in accordance with Part C of this Policy.
e. Authorised CCTV Operator - means a person authorised by the Director, Operational Services, Division of Facilities Management (or delegate) to view Closed Circuit Television System (CCTV) images or footage, live or recorded, for security, safety and/ or access purposes.

f. Campus Security Personnel - means any person engaged by the University to provide security services or traffic control functions in relation to University premises.
g. Card - for the purposes of this Policy the word 'card' may be extended to include codes or personal identification numbers (PIN) used for access purposes.
h. Closed Circuit Television System (CCTV) includes 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 Division of Facilities Management CCTV design and installation specification.
i. Controlled Area - means any area or space on University premises to which general or public access is not available at any designated time.
j. Critical Assets - means any University equipment, infrastructure, documents or intellectual property, the loss of which would seriously impact on the activities of the University.
k. Head Contractor/Principal Contractor – Is a person or entity that has the management or control of defined construction workplace as defined under the Work Health and Safety Act 2011 No 10 (NSW).
l. 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, University security control room, automatic SMS, voice message or visual alarm forwarding system which will communicate system alerts and facilitate appropriate responses to alarms.
m. Security - means the security office of each campus and any Campus Security Officer, Manager or Security Officer.
n. Security Incident - means any situation arising that may compromise the security of people, assets or property on a University premises, 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.
o. Security Licence - means an appropriate licence granted under the Security Industry Act 1997 No 157 or the Security Industry Regulation 2016 or equivalent legislation in any other relevant jurisdiction.
p. Security Management - means Manager, Campus Services, the Manager, Operational Services and the Director, Operational Services within the Division of Facilities Management who are employed by the University to manage security operations and Security.
q. 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.
r. 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.
s. University Premises - means 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.
t. University Rules - means the Charles Sturt University Act 1989 No 76, Charles Sturt University By-law 2005, rules, regulations, policies, guidelines, and procedures, applying to students, staff, and visitors.
u. Visitor - means any person who is not a University student or member of staff but who accesses University premises, including contractors to the University and members of the public.

Section 3 - Policy

Part A - Access to University Premises

(7) Persons with a valid reason may enter University premises, provided that:

a. entry has not been prohibited by any Authorised Access Officer; and,
b. they comply with any relevant policies or procedures applicable to their right of access to the University premises.

(8) All staff and students and applicable contractors are issued with university identification cards which must be:

a. carried during attendance on University premises, and
b. shown in response to any reasonable request from any Authorised Access Officer or any other member of staff who might require such identification in the course of their duties.

Incidents and Emergencies

(9) This Policy does not limit 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.

(10) Emergency Services may, from time to time, conduct specific operations on University premises.

(11) Any member of Security who calls the Emergency Services to University premises must immediately inform a member of Security Management. Depending upon the nature of the event, the Chief Warden may enact the Critical Incident Response Group Procedure.

(12) In the event of the Emergency Services being called to attend an emergency on University premises by any staff, student or visitor, the person instigating the call must inform a member of Security as soon as possible advising the nature of the emergency to allow Security to coordinate and expedite Emergency Services attendance.

(13) A head contractor in control of a building site is required to have emergency arrangements in place.

Controlled Areas

(14) An Authorised Access Officer may designate a controlled area to regulate access within University premises to ensure the security and safety of people and university property.

(15) Controlled Areas are identified by:

a. signs;
b. locked doors;
c. fences;
d. boom-gates;
e. barrier tape; or
f. defined by the instruction of campus Security personnel or an authorised member of staff.

(16) Persons must not access a controlled area without approval by an Authorised Access Officer.

Access Control Devices

(17) Access control devices are issued by the University to allow students, staff, and approved visitors access to controlled areas of the University. These must be used in accordance with any accompanying instructions and shall:

a. not be interfered with under any circumstances;
b. only be used to enter controlled areas for which they are currently authorised;
c. only be used 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; and,

d. remain the property of the University and must be returned on demand at any time.

(18) Unauthorised possession, use or tampering of an access control device by staff or students, shall be deemed to have committed a breach of discipline or misconduct under the relevant University Policy, in particular, the Staff Code of Conduct and Student Misconduct Rule 2020.

(19) The selection, installation, maintenance and operation of all access control devices and associated equipment at University premises must be made in consultation with, and seek final approval from the Division of Facilities Management.

(20) To ensure compliance with applicable fire and building safety codes, non-university approved access control equipment, including mechanical keys or locks, must not be used.

(21) Any unauthorised fabrication, duplication, issuing, possession, or use of access control devices is strictly prohibited. Fabrication of any access control devices must only be performed after written approval from the Division of Facilities Management.

Monitoring Access and Safety

CCTV

(22) 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 premises.

(23) Only CCTV equipment that meets the Division of Facilities Management's Operational Design Standards shall be applied to University premises.

(24) Appropriate standard operating procedures shall be applied to all security CCTV applications to ensure effective and ethical management of equipment. Recorded information is appropriately maintained and accessed by authorised CCTV operators. All security CCTV systems installed will comply with the following:

a. located in a secure area;
b. signage installed in accordance with the legislation of the relevant State or Territory;
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. used in accordance with any relevant legislation or applicable codes of practice.

Alarm Systems

(25) The Division of Facilities Management has responsibility for selection, installation and maintenance of all alarm systems on University premises.

(26) University property containing critical assets, highly confidential or sensitive information will be considered for protection by a suitable monitored alarm system.

(27) Staff performing tasks which may be accompanied with a higher than usual security related risk may (as part of an overall security solution) be considered for protection by a suitable monitored alarm system, such as a personal duress alarm.

(28) All staff, students and visitors are responsible for considering their own environmental security issues and are encouraged to seek professional advice from the Division of Facilities Management regarding the most appropriate

security solutions. This may include alarm systems such as personal duress alarms.

Part B - Disorderly Conduct

(29) Disorderly conduct is recognised as general misconduct and subject to relevant University Rules governing misconduct, for example, the Charles Sturt University Enterprise Agreement, Student Misconduct Rule 2020 and the Code of Conduct.

(30) The following forms of conduct will be considered 'disorderly conduct' and may lead to action being taken by Authorised Access Officers:

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. threatening the health, safety or welfare of staff, students or visitors of the University;
d. willfully failing to obey any reasonable direction of Authorised Access Officers in relation to University premises, access and order;
e. failing to provide appropriate identification on request by an Authorised Access Officer;
f. willfully entering any place on University premises which the person is forbidden to enter;
g. willfully littering, 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.

Reporting Disorderly Conduct

(31) In the occurrence of an alleged act of disorderly conduct which poses a threat or risk to personal safety, or which requires immediate intervention; staff, students and visitors must contact Police and Security immediately.

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

(33) Complaints regarding alleged disorderly conduct by staff that requires Security intervention, must be reported to the Division of People and Culture as soon as practicable after the alleged misconduct has occurred by Security.

(34) Complaints regarding alleged disorderly conduct against visitors must be reported to Security. Security shall notify the Head of Campus as soon as practicable after the alleged misconduct has occurred.

Part C - Responsibilities

Security Incidents

(35) All security incidents which occur on University premises must be reported to Security.

(36) Security is responsible for ensuring Police are notified of all incidents on University premises where appropriate, including those relating to the loss or damage of university property.

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

Division of Facilities Management

(38) Division of Facilities Management are responsible for the administration of access to University premises

including:

a. maintaining the security and safety of University premises;
b. providing access to common areas, such as learning commons and timetabled teaching spaces;
c. managing the University's access control systems which provide access to controlled areas;
d. promoting uniformity and compatibility of access control devices used at University premises and for the maintenance of central records; and
e. providing adequate training for access coordinators.

Security Staff

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

(40) Security staff will fulfill their duties in a lawful, fair and equitable manner without damage to the University's reputation or unfairly impinging on the rights of individuals.

(41) Security staff will take reasonable action to assist with:

a. maintaining public order on University premises;
b. the prevention and investigation of crimes against an individual on University premises and report suspected crimes to the Manager, Campus Services , Division of Facilities Management the Police and other relevant external authorities. Crimes such as:
    i. assaults;
    ii. offensive behaviour;
    iii. indecent exposure; or
    iv. trespass etc.
c. the prevention and investigation of property crimes on University premises and report suspected crimes to the Manager, Campus Services , Division of Facilities Management , the Police and other relevant external authorities. Crimes such as:
    i. willful damage;
    ii. theft; and
    iii. burglary.
d. managing emergencies and critical incidents, including reporting emergencies to the Manager, Campus Services , Division of Facilities Management, Police, Fire, Ambulance and other relevant external authorities. Emergencies such as:
    i. fires;
    ii. chemical spills; and
    iii. injuries.
e. providing information and assistance to the public in the circumstance where Security are the first and possibly only available contact for the University; and
f. ensuring staff, students and visitors comply with the law and University Rules whilst on University premises.

Security Master License

(42) The Security Industry Act 1997 No 157 requires the University to maintain a current Security Master Licence where it directly 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 is the only person who can authorise the employment of Campus Security Officers.

(43) Under no circumstances shall any persons be employed or engaged by the University as a member of Security without the written consent of the Security Master Licence holder, Director, Operational Services, Division of Facilities Management.

Authorised Access Officers

(44) Authorised Access Officers are invested with the authority to make enquiries and take reasonable action, in compliance with this Policy and associated documentation, to regulate the access and behaviour of staff, students and visitors. This includes:

a. requesting any person on University premises to produce proof of identity;
b. making reasonable and necessary enquiries to validate an individual's status if they are unable to produce their university identification card or otherwise justify their right to be on University premises;
c. requesting any staff, student or visitor to leave University premises if:
    i. they are unable to produce appropriate identification or justification for being on University premises;
    ii. the Authorised Access 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;
    iii. the person is involved in disorderly conduct (see Part B Disorderly Conduct); or,
    iv. 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 staff, students or visitors on University premises.

(45) Authorised Access Officers are invested with the authority to administer and control vehicle access to University premises and the traffic and parking provisions therein.

(46) Authorised Access Officers are responsible for appointing Access Coordinators for their area of responsibility.

(47) Authorised Access Officers will call Police for assistance where any person refuses to comply with a request to leave the University premises.

(48) It is expected that all Authorised Access Officers are fully conversant with relevant standard operating procedures prior to commencing duties at the University and throughout their employment.

(49) Authorised Access Officers must have their university identification card or security licence prominently displayed at all times or be able to produce this on demand.

Access Coordinators

(50) Access Coordinators are appointed by the relevant Authorised Access Officer and have authority to grant, deny or revoke access privileges to controlled areas for which the Faculty, Division or Centre is directly responsible.

(51) Access Coordinators are responsible for:

a. managing access control devices within their allocated space in accordance with this Policy, and
b. managing internal access within the allocated space, as per the Space Management Policy under the direction of the Access Coordinator's senior manager.

Supervising Staff Members

(52) Supervising staff members are responsible for those under their control. This may include other staff, visitors (including contractors) or students.

(53) Supervising staff members are responsible for ensuring approved persons are inducted and supervised into

controlled areas. They must also provide instruction and supervision at a level that maintains the security of the area, safety of staff, students and visitors; and protection of university property.

(54) Supervising staff members who witness disorderly conduct by students, staff, visitors (including contractors) on University premises, must:

a. request the individual(s) to discontinue the disorderly conduct;
b. request the individual(s) to leave the area;
c. contact the Police and Security for further assistance if the individual(s) refuse to comply; and
d. report each incident in accordance Part B - Disorderly Conduct.

Section 4 - Procedures

(55) Nil

Section 5 - Guidelines

(56) Nil

Status and Details

Status	Current
Effective Date	20th July 2018
Review Date	20th July 2023
Approval Authority	Executive Director, Division of Facilities Management
Approval Date	13th July 2018
Expiry Date	Not Applicable
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 Division of Facilities Management +61 2 69332286