EM Security & Traffic Design Standard

Version	Approved by	Approval date	Effective date	Next full review
1.0	Executive Director, Estate Management	August 2019	September 2019	September 2022

Standard Statement	
Purpose	The Security & Traffic Management Design Standard outlines the minimum requirements for the design, construction and maintenance of security systems at UNSW. It ensures new and refurbished buildings/spaces are designed to meet the objectives of the university, have applied CPTED principles, the desired level of physical security controls to mitigate identified risks, use quality materials that are environmentally sustainable, and are cost efficient to maintain and operate. This document supports the UNSW Security Systems Installation Specifications
Scope	Applies to all UNSW owned and operated properties, including occupied buildings, car parks, sport and recreational facilities, pathways, roadways
Standard	

1. Design Details

1.1. Design Framework

UNSW Security & Traffic Management Design Standards and Security Systems Installation Specifications form a part of the broader UNSW EM Design & Construction Standards & Guidelines. These design standards are to be followed during the design phase of all building and refurbishment projects at UNSW.

As each construction/refurbishment project is unique, it is essential that a security threat and vulnerability assessment is undertaken to identify the risks in relation to people, property and assets to ensure the security controls applied are sufficient and not over engineered. For new construction, the ongoing operations of the building and its users is essential in determining the security measures to be implemented.

The design consultants are to provide a CPTED plan which will be reviewed and endorsed by the UNSW Head of Security & Traffic.

Any proposed variations to the approved security design concept must undergo re-approval in consultation with UNSW Head of Security & Traffic.

1.2. UNSW Security Technical Specification

All installations must be carried out in accordance with UNSW Security Systems Installation Specifications, manufacturer specifications and data sheets, to ensure product performance over its intended life span and so as not to invalidate any warranties.

1.3. Preferred Security Contractors

All installations and/or modifications to the UNSW security system must be performed by approved preferred security contractors.

The preferred security contractors list can be obtained from EM Security Services (security.services@unsw.edu.au).

2. Definitions and Acronyms

EM	Estate Management
CPTED	Crime Prevention Through Environmental Design
CCTV	Closed Circuit Television
Gallagher	UNSW security access control system
CATS	Centrally Allocated Teachings Spaces

3. CPTED Strategies

The design and planning of University buildings and facilities will aim to:

a) increase the effort required to engage in criminal or anti-social behaviour;

b) increase the perceived risk of engaging in criminal or anti-social behaviour;

c) reduce the rewards from a criminal or anti-social act; and

d) reduce the availability of excuses for criminal or anti-social behaviour.

e) encourage occupants to take ownership of their designated space

f) encourage social engagement

This will be achieved by applying CPTED strategies during the concept design stage;

3.1. General

The University requires attention towards the environment to complement and enhance the security of the campuses. Crime Prevention Though Environmental Design is an approach to preventing crime where its objective is to improve security by limiting criminal opportunity through the use of natural barriers and natural surveillance. Where possible, the University prefers CPTED to be used in conjunction with traditional electronic, mechanical, and structural crime prevention techniques. When conducting security related work, consideration shall be given to the following:

3.2. Territoriality

Territorial reinforcement of an area is the physical design that helps develop a sense of territoriality by the user that produces a perceived risk to an intruder. This shall be achieved through the use of clearly defined perimeters by way of barriers (fences, hedges or rows of trees) and other visual indicators (changes in ground lay material, lighting levels or wide-open spaces). Where applicable, the security designer shall demonstrate territoriality in instances that require the restriction of individuals.

3.3. Natural Surveillance

Keeping intruders under observation will result in a higher perception of detection. This shall be achieved by techniques that minimise the opportunities for intruders to conceal themselves and their actions. Large glass windows, well-kept gardens, lighting and wideopen spaces will increase the natural surveillance of an area. The effectiveness of electronic CCTV systems is further increased when natural surveillance techniques are employed. Where applicable, the security designer shall demonstrate natural surveillance particularly in the vicinity of CCTV cameras.

3.4. Natural Access Control

The prevention of access to an area and the creation of the perception of detection and increased effort required by an offender constitutes Natural Access Control. Lighting can be employed to control the movements and concentrations of people. Individuals will be attracted to brightly-lit areas at night. Natural Access Control shall be utilised to provide an increased level of safety for authorised individuals.

4. Risk Assessment

The risk assessment will be based on the facility characterisation and the threat and vulnerability assessment. This will provide basis of the criticality level of security for the people, property and assets within that location.

5. Security Zones

Security Zones provide a methodology for physical security mitigation based on the security risk assessment. The primary outcomes of the zones methodology are to give a scalable level of protection from:

- unauthorised or covert access, and
- forcible attack.

Table 1 below provides broad descriptions of the functions in the Zones, the information and assets they can handle and store in the Zones, and some examples of Security Zones.

Table 1:

Zone type	Description	Examples
Zone One Public	Public zones are normally accessible to everyone with no automatic ability to impose access control measures. Information and assets if compromised are low level impact to business operations	• External Open Space • Car parks • Pedestrian corridors and roads
Zone two Semi-Public	Access to these areas is typically restricted outside normal business hours. Visitors are considered guests of the building and their access maybe limited at any time. Information and assets if compromised are low level impact to business operations	• Building foyers – common spaces • Centrally Allocated Teaching Space
Zone Three Semi-Private	Semi-Private areas are predominantly for the use of limited, authorized persons. Visitors may enter but are either invited or screened prior to entry. Facilities deploy electronic access control or procedural access control measures to limit free access beyond a control point. Information and assets if compromised are medium level impact to business operations	• Concierge/staffed receptions/Service Counters • Gym • Childcare • Event Space • Licensed premises • Retail • Library
Zone Four Private	Private areas are limited to access by authorized individuals and visitors are escorted within those areas. Information and assets if compromised are medium level impact to business operations	• Residential

Zone Five Restricted	Restricted areas are private areas that contain critical research and infrastructure, essential services or sensitive assets or reserved for executive. Access is limited to core users only. Information and assets if compromised are high level impact to business operations	• Data Centres • IT Service Rooms • Research Labs – PC1, PC2 & PC3 • Security Control Room • Chancellery Executive • Plant Rooms

6. Security Layers

The above zones should be applied to the design to understand what security control measures are required. Buildings can have multiple zones dependent on the function, increasing the protection with each new zone.

Example of layering zones below:

7. Security Controls

The UNSW Security Team, including Operations Managers and Head of Security will provide input on level of security controls required in each zone, including access control, intruder detection systems, duress alarms, CCTV, Help Points, vehicle control and hostile vehicle mitigation. The minimum level of controls is outlined below for each zone;

Zone One	Zone Two	Zone Three	Zone Four	Zone Five
CCTV Help Point* Vehicle control and hostile vehicle mitigation Signage	CCTV Access Control Signage	CCTV Access Control Intruder Detection Systems Duress** Signage	CCTV Access Control to single door and office area Signage	CCTV Access Control (Biometric/Dual Authentication) Intruder Detection Systems

				Duress**

Accountabilities	
Responsible Officer	Head of Security and Traffic, Estate Management
Contact Officer	Security Operations Manager, Systems
Supporting Information	
Legislative Compliance	This Standard has been developed in accordance with State and NSW Legislation, State Government Guidelines and Australian and New Zealand Standards. These include but not limited to: • *Australia and New Zealand Risk Management Standard AS/NZS ISO 31000:2009.* • *NSW Crime Prevention Through Environmental Design (CPTED) Guidelines* • *AS/NZs 2201:1:207 Intruder Alarm Systems* • *AS 4806.1.2006 Closed Circuit Television (CCTV)* • *National Security – Protecting Crowded Places from Terrorism* • *Hostile Vehicle Guidelines for Crowded Places* • *Work Place Surveillance Act 2005*
Related Documents	UNSW Security Systems Installation Specifications
Superseded Documents	Nil
File Number	RAMS Document number