Revision 1.0

Infrastructure Design Standards

Module S18: Security Systems

Division of Finance (Strategic Infrastructure)
Charles Sturt University

Document Control

Document Name	**Infrastructure Design Standards**
Sub-Section Name	**Module S18: Security Systems**
Document Status	current
Revision Number	1.0
Effective Date	11/11/2024
Review Date	10/11/2025
Unit Head	Director, Strategic Infrastructure
Author(s)	The Standards have been developed by Strategic Infrastructure, Facilities Management, external consultants, contractors, and colleagues.
Enquiries Contact	Division of Finance (Strategic Infrastructure)

Contents

1. Introduction 4
1.1. Overview 4
1.2. The University 4
1.3. University Vision and Values 4
1.4. Using the Infrastructure Design Standards 5
1.5. Modules 5
1.6. Related Documents 6
1.6.1. University Documents 6
1.6.2. Federal Legislation 6
1.6.3. NSW State Legislation 7
1.6.4. Federal Regulations and Standards 7
1.6.5. NSW State Regulations and Standards 7
1.6.6. Manufacturer Specifications and Data Sheets 7
1.6.7. Project-Specific Documents 7
1.7. Discrepancies 8
1.8. Departures 8
1.9. Professional Services 8
1.10. Structure of Document 8

2. General Requirements 9
2.1. Overview 9
2.2. Guiding Principles of Security and Privacy 9
2.2.1. Compliance with Australian Standards and Legislation 9
2.2.2. Core Principles 10
2.2.3. Risk Management and Business Resilience 10
2.2.4. University Security Plan 11
2.2.5. Physical Security Ratings 11
2.2.6. Crime Prevention Through Environmental Design 12
2.3. Communication & Switching Components 12
2.4. Certification 13
2.5. Certification Criteria 13
2.5.1. Certification Process 13
2.6. Boom Gates 14
2.7. Defects Liability Period 16

3. Supporting Documentation 18
3.1. Supporting Legislation 18
3.2. Supporting Standards 18
3.3. Industry Codes of Practice 20
3.4. Related University Policy 20
3.5. Other Resources 21

1. Introduction

1.1. Overview

The Charles Sturt University Infrastructure Design Standards (the Standards) outline the University's expectations for its built forms to achieve consistency in the quality of the design and construction of those built forms.

The Standards have been developed to provide guidance to the design team and to assist Facilities Management to drive a consistent approach to the design, construction, commissioning, handover, and operation of new capital projects to ensure the new asset is fully integrated into campus life and conforms to the University's standards and policies.

The successful integration of any new project into the day-to-day operation of campus life cannot be underestimated and is vital to ensuring the new asset provides a fully functional platform for Facilities Management clients and the University. The Standards will ensure Facilities Management is successful in supporting the University's strategic objectives now and into the future. The pitfall of viewing any new project as a standalone entity must be avoided as any new project is an extension of the existing campus.

The Standards are aligned with Charles Sturt's requisites for aesthetic appeal, life cycle maintenance and environmental sustainability, while ensuring that there is sufficient scope for innovation and technological advancements to be explored within each project.

1.2. The University

The history of Charles Sturt University dates to 1895, with the establishment of the Bathurst Experiment Farm. Formed progressively through the merge of regional institutions in south-western and western NSW, Charles Sturt was formally incorporated on 19 July 1989 under the Charles Sturt University Act 1989. As one of Australia's newer universities, Charles Sturt has been built on a tradition of excellence in teaching and research spanning more than 100 years.

With over 40,000 current students studying both on-campus and online, Charles Sturt University is the largest tertiary education institution in regional Australia. The University operates six main campuses across New South Wales in Albury-Wodonga, Bathurst, Dubbo, Orange, Port Macquarie, and Wagga Wagga, alongside specialist campuses in Canberra, Parramatta, and Goulburn. Charles Sturt University is structured around three Faculties: Arts and Education; Business, Justice and Behavioural Sciences; and Science and Health.

1.3. University Vision and Values

Charles Sturt University is committed to building skills and knowledge in its regions by offering choice and flexibility to students, while collaborating closely with industries and communities in teaching, research, and engagement. As a significant regional export industry, the University brings both strength and learning back to its regions, positioning itself as a market-oriented institution. Its goals are to remain the dominant provider of higher education in its regions and a sector leader in flexible learning.

Charles Sturt University believes that wisdom has the power to transform communities. With perseverance and dedication, the University contributes to shaping resilient and sustainable regions for the future. Acknowledging the deep culture and insight of First Nations Australians, the University's ethos is encapsulated by the Wiradjuri phrase *yindyamarra winhanganha,* which translates to "the wisdom of respectfully knowing how to live well in a world worth living in." Through its values, Charles Sturt University fosters a welcoming community and learning environment that supports innovation, drives societal advancement, and gives back to the regions it serves.

1.4. Using the Infrastructure Design Standards

The Infrastructure Design Standards are written to advise Charles Sturt University performance requirements and expectations that exist above and beyond existing industry codes and standards.

The Infrastructure Design Standards do not repeat codes and standards.

Performance to Codes and Standards are a non-negotiable regulatory minimum of any design solution, to be determined for each project by the design team.

The Standards are to be used by all parties who are engaged in the planning, design, and construction of Charles Sturt's facilities. This includes external consultants and contractors, Charles Sturt's planners, designers, and project managers as well as faculty and office staff who may be involved in the planning, design, maintenance, or refurbishment of facilities. All projects must comply with all relevant Australian Standards, NCC, EEO as well as Local Government and Crown Land Legislation.

1.5. Modules

The Standards are divided into the following modules for ease of use, but must be considered in its entirety, regardless of specific discipline or responsibilities:

- S01 Overview and Universal Requirements
- S02 Active Transport
- S03 Acoustics
- S04 Building Management System
- S05 Electrical and Lighting
- S06 Energy Management
- S07 Ergonomics
- S08 Fire and Safety Systems
- S09 Floor and Window Coverings
- S10 Furniture
- S11 Heritage and Culture
- S12 Hydraulic

- S13 Information Technology
- S14 Irrigation
- S15 Mechanical Services
- S16 Roof Access
- S17 Termite Protection, Vermin Proofing and Pest Management
- **S18 Security Systems**
- S19 Signage
- S20 Sustainable Building Guidelines
- S21 Waste Management
- S22 Project Digital Asset and Data Requirements
- S23 Commissioning, Handover and Training

1.6. Related Documents

1.6.1. University Documents

The Standards are to be read in conjunction with the following relevant University documents, including but not limited to:

- Facilities and Premises Policy along with supporting procedures and guidelines
- Charles Sturt University Accessibility Action Plan 2020 - 2023
- Relevant operational and maintenance manuals
- Charles Sturt University Asbestos Management Plan
- Charles Sturt University Signage Guidelines
- Charles Sturt University Modern Slavery Statement
- Charles Sturt University Sustainability Statement
- Charles Sturt University Work Health and Safety Policy
- Charles Sturt University Risk Management Policy
- Charles Sturt University Resilience Policy
- Charles Sturt University Health, Safety and Wellbeing Policy

1.6.2. Federal Legislation

The planning, design and construction of each Charles Sturt University facility must fully comply with current relevant Federal legislation, including but not limited to:

- National Construction Code (NCC)
- Disability Discrimination Act 1992 (DDA)
- Environment Protection and Biodiversity Conservation Act 1999 (EPBC)
- Work Health and Safety Act 2011

1.6.3. NSW State Legislation

The planning, design and construction of each Charles Sturt University facility must fully comply with current relevant Federal legislation, including but not limited to:

- Work Health and Safety Act 2011
- Environmental Planning and Assessment Act 1979 (EP&A Act)
- Building and Development Certifiers Act 2018
- Heritage Act 1977
- Protection of the Environment Operations Act 1997 (POEO Act)
- Design and Building Practitioners Act 2020
- State Environmental Planning Policies (SEPPs)
- Local Government Act 1993

1.6.4. Federal Regulations and Standards

- Relevant Australian or Australian/New Zealand Standards (AS/NZS)
- Safe Work Australia Model Codes of Practice
- Work Health and Safety Regulations 2011
- Disability (Access to Premises – Buildings) Standards 2010
- National Environment Protection Measures (NEPMs)

1.6.5. NSW State Regulations and Standards

- SafeWork NSW Codes of Practice
- Disability (Access to Premises – Buildings) Standards 2010
- Building and Development Certifiers Regulation 2020
- NSW Work Health and Safety Regulation 2017
- Protection of the Environment Operations (General) Regulation 2022
- NSW State Environmental Planning Policies (SEPPs)
- Fire and Rescue NSW Fire Safety Guidelines
- NSW Local Council Development Control Plans (DCPs)

1.6.6. Manufacturer Specifications and Data Sheets

All installation must be carried out in accordance with manufacturer specifications and data sheets to ensure product performance over its intended life and so as not to invalidate any warranties.

1.6.7. Project-Specific Documents

Requirements specific to a particular project, campus, or other variable, will be covered by project specific documentation, such as client briefs, specifications, and drawings. These Standards will supplement any such project specific documentation. The Standards do not take precedence over any contract document, although they will typically be cross-referenced in such documentation.

Extracts from the Standards may be incorporated in specifications; however, it must remain the consultant's and contractor's responsibility to fully investigate the needs of the University and produce designs and documents that are entirely 'fit for purpose' and which meet the 'intent' of the project brief.

1.7. Discrepancies

The Standards outline the University's generic requirements above and beyond the above-mentioned legislation. Where the Standards outline a higher standard than within the relevant legislation, the Standards will take precedence. If any discrepancies are found between any relevant legislation, the Standards and project specific documentation, these discrepancies should be highlighted in writing to the Manager, Capital Works.

1.8. Departures

The intent of the Standards is to achieve consistency in the quality of the design and construction of the University's built forms. However, consultants and contractors are expected to propose 'best practice / state of the art' construction techniques, and introduce technological changes that support pragmatic, innovative design. In recognition of this, any departures from relevant legislation, or the Standards, if allowed, must be confirmed in writing by the Manager, Capital Works. Any departures made without such written confirmation shall be rectified at no cost to the University.

1.9. Professional Services

All projects at Charles Sturt University require the involvement of adequately skilled and experienced professionals to interpret and implement the Standards. Consultants or contractors lacking proper qualifications and licenses are not permitted to conduct any work.

1.10. Structure of Document

This document is structured into 4 sections:

Section 1 Introduction (this Section).

Section 2 General Requirements – outlines the general requirements or design philosophies adopted at Charles Sturt University.

Section 3 Supporting Documentation – Legislation, Standards, Codes of Practice, University Policies, and other applicable technical references.

Section 4 Specifications (if applicable) – materials specifications and/or preferred lists for materials, processes or equipment used by Charles Sturt University.

2. General Requirements

2.1. Overview

This module sets out the essential criteria for electronic security design in both new construction projects and upgrades to existing buildings at Charles Sturt University. It highlights the importance of establishing a comprehensive building security framework during the initial design phase of each project. Central to this approach is a detailed risk assessment, conducted in collaboration with the University's Chief Security Officer and other key stakeholders. These assessments identify potential security threats, which form the basis for developing a comprehensive security concept.

Once the security concept is established, the appointed design consultant is responsible for creating detailed specifications. These specifications must integrate seamlessly with other sections of the university's Design Standards, including Electrical Services, Fire Protection and Detection Systems, External and Internal Building Elements, and Telecommunication Networks. Compliance with all relevant codes, standards, and best practices is mandatory throughout the design process.

This section of the Design Standards focuses specifically on physical security measures aimed at preventing, detecting, and mitigating unauthorized activities on university premises. It does not cover Information Technology security measures, which are outside the scope of this document.

Charles Sturt University is committed to ensuring a safe and secure environment for its staff, students, and visitors. The university's security policies provide a framework for managing security and safety across all campus buildings and external spaces.

2.2. Guiding Principles of Security and Privacy

Charles Sturt University acknowledges the critical role that Video Surveillance and Security Systems (VSSS) play in ensuring campus safety and security. However, these systems must strike a careful balance between addressing security needs and respecting individual privacy rights. In developing and implementing security standards, the university recognizes the need to thoughtfully navigate potentially conflicting interests.

The university's approach to video surveillance focuses on strategic deployment in high-risk areas where the potential for criminal activity is greater. This targeted strategy enhances campus security without unnecessarily intruding on personal privacy. Unlike blanket surveillance, which could negatively impact creativity and freedom of expression, the university prioritizes both security and privacy, aiming to protect faculty, staff, students, and visitors.

2.2.1. Compliance with Australian Standards and Legislation

Charles Sturt University ensures that all CCTV installations and practices fully comply with Australian Standards and relevant Commonwealth and State privacy legislation, such as the National Privacy Principles (NPPs) under the Privacy Act 1988 (Cth) and the NSW Privacy and Personal Information Protection Act 1998 (NSW). Key principles guiding these practices include:

- **Necessity and Proportionality**: CCTV systems are implemented only to address legitimate security needs, with measures that are proportional to the identified risks.
- **Transparency and Accountability:** The university maintains clear policies for the operation and management of CCTV systems, ensuring transparency in the purpose, use, and storage of surveillance data.
- **Privacy Impact Assessment (PIA):** Prior to deploying surveillance systems, comprehensive PIAs are conducted to assess and mitigate any potential privacy concerns.
- **Data Security and Access Control:** Strict security protocols safeguard recorded footage, with access limited to authorized personnel only.
- **Retention and Disposal:** Recorded surveillance data is retained only for as long as necessary to achieve its intended purpose and is securely disposed of according to the university's data retention policies.

2.2.2. Core Principles

The security systems at Charles Sturt University follow several key guiding principles to ensure a robust and future-ready infrastructure:

- **Risk-Based Approach:** All security designs are based on comprehensive risk assessments, identifying critical assets and their associated threats. Each space must be classified based on risk, and the appropriate security measures (electronic access control, CCTV, alarms, etc.) must be deployed accordingly.
- **Layered Security:** The security strategy is tiered, combining physical, electronic, and procedural measures to protect against unauthorized access and to detect, delay, and deter potential security breaches. This includes creating a series of security "zones" (e.g., public, restricted, sensitive), each with progressively stronger security measures.
- **Compliance with Standards:** University security infrastructure must comply with Australian standards (such as AS 2201 for security alarms and AS 3745 for emergency evacuation systems) and applicable state legislation. Compliance ensures legal adherence and protection against liability.
- **Continuous Improvement:** The University follows a continuous improvement model for security, regularly updating systems to integrate the latest technological advancements and reflect lessons learned from incidents.

2.2.3. Risk Management and Business Resilience

Risk management and the development of a resilient business model are foundational to our security designs and standards. All essential systems are integrated within a comprehensive, organization-wide security framework, such as the Protective Security Policy Framework (PSPF), to ensure holistic management of security risks. This approach allows for a unified strategy that aligns security measures across the university.

2.2.4. University Security Plan

This document supports and complies with the University Security Plan (USP) and is designed to implement set controls defined by that document. Whilst it is a security in confidence document, approval to share the below has been granted. Each space we assess for Essential Systems requirements, will apply one of the zones below to inform the risk context and how that converts to application of Essential Systems.

Zone + Colour	Name	Definition
A	Public	Areas that are university property but public access. This includes the vast bulk of the university's outdoor areas and numerous indoor areas. Level 4 classified documents.
B	Authorised	Areas accessible for authorised people only. Includes all staff, students and signed in visitors and contractors. Level 3 classified documents.
C	Staff only	Dedicated staff work areas, the bulk of office rooms and areas within the university. A 'need to access' principle is in place, and not all staff have access. Level 2 classified documents.
D	Restricted	Areas where critical assets have been identified and with tailored security requirements in place. Access to be auditable. Example, research data, essential FM or DIT infrastructure or office areas of executive staff. Level 1 classified documents.

2.2.5. Physical Security Ratings

Each type of physical control is given a rating to show how it affects risk reduction. This matches the PSPF ratings for consistency

Rating + Colour	**Meaning**	**Examples**
1	Excellent controls, automation, live monitoring, suitable for critical infrastructure	Gallagher Access Control, Video Surveillance, Alarm systems
2	High controls, monitoring and audit and some automation	Aperio Access Control, general alarms
3	Medium controls, but little or no audit or awareness capacity	Salto Access control, 3rd party readers, unmanaged alarms
4	Some controls, usually physical or mechanical	Master Key System
5	Lowest level, and is generally to a domestic level, non-electronic, uncontrolled	No keys, unmanaged keys

2.2.6. Crime Prevention Through Environmental Design

The principles of Crime Prevention Through Environmental Design (CPTED) are administered in NSW by the NSW Police. This international multi-disciplinary approach uses urban and architectural design and the management of built and natural environments for crime prevention.

CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants so they can gain territorial control of areas, reduce crime, and minimize fear of crime.

It should be applied in combination with Essential systems to enhance the effectiveness of those systems. The bold items are specifically relevant to essential systems itself.

- Territorial reinforcement – visible space ownership, care, signage, boundary marking and used space not abandoned.
- Surveillance
    - Natural – visible line of sight, passive view from multiple locations, no hide points, lighting, well maintained and used.
    - Technical – cameras, help points, and mirrored building panels.
    - Formal– security guards or on-site supervisors
- Access control
    - Natural – landforms, waterways, building configuration, pathways, landscaping, fencing and gardens.
    - Technical – access control systems, electronic key-safes, kiosks and monitoring
    - Formal - security guards or on-site supervisors
- Space and activity management – well planned and designed areas for maximum application for the previous elements, safe areas, natural flow between spaces, design of public and secure area separation.

2.3. Communication & Switching Components

The communication infrastructure for the CCTV system is managed by the Division of Information Technology (DIT). DIT is responsible for supplying the necessary hardware, network connections, and ongoing maintenance of network equipment.

It is the Project Officer’s responsibility to coordinate with the contractor and DIT regarding any network requirements. This includes providing DIT with installation timelines for any additional network equipment and identifying any associated costs during initial design. Furthermore, the contractor must ensure that the IP CCTV system design complies with the latest version of the CSU Specification for Voice and Data.

Refer to Module S13 Information Technology for additional information.

2.4. Certification

Certification is a cornerstone in ensuring that all security systems installed meet the highest quality standards, handled by experienced and certified specialists. Given the complexity of Charles Sturt University's systems, elevated levels of certification and expertise are imperative. Trainees or technicians lacking sufficient familiarity with these advanced systems are deemed unsuitable. Certification records are managed through the Gallagher system, covering both individual technicians and companies. Approved vendors and personnel are detailed in the "Authorised Vendors and Technicians – Essential Systems" document.

2.5. Certification Criteria

The following criteria govern the certification process for personnel and companies working on essential systems:

- Compliance with legislative requirements
- Possession of necessary licenses and qualifications
- Adherence to industry association and Australian Standards
- Meeting manufacturer-specific standards and qualifications
- Alignment with university-specific standards, policies, and procedures
- Demonstrated experience in handling enterprise-level systems
- Completion of relevant qualifications from an RTO (e.g., TAFE) or university
- Fulfillment of certifier-specific requirements

2.5.1. Certification Process

Comprehensive details about the certification process are outlined in the associated documentation. The process ensures alignment with CSU’s stringent requirements, from initial assessment to final approval.

Certification Terms

Integration: Covers APIs, middleware, and all interconnected systems.

Works: Refers to any tasks associated with system operations or modifications.

Aperio Certification

All Aperio systems must integrate seamlessly with Gallagher, requiring certifications listed in Section 2.5. Though formal Aperio certifications are pending, relevant experience with enterprise-level systems (e.g., managing 500+ readers within a Gallagher framework) is essential.

Avigilon Alta Certification

Technicians must have experience with enterprise-level systems managing over 500 cameras. CSU partners with Stax Security for Avigilon Alta hardware and licensing, with the current contract valid until December 2024.

Avigilon Unity Certification

This legacy system has transitioned to Avigilon Alta.

Gallagher Certification

All work involving Gallagher systems requires verified certifications, particularly for enterprise setups (500+ readers, 50+ controllers). Expertise in complex system environments is mandatory.

Salto Certification

Salto installations linked to Gallagher must meet the certification requirements in Section 2.5, alongside specific Salto credentials. As a legacy system, Salto is now restricted to Energy Saving Device management.

Torus Certification

Certification for Torus systems mandates experience in managing enterprise environments with at least 10 integrated key cabinets.

Security Works and Licensing

A Class 2C Security License is compulsory for work on security equipment. For queries, consult the NSW Police Security Licensing Enforcement Directorate (SLED).

Cabling and ACMA Licensing

All essential system tasks involving devices like Salto and Aperio require an ACMA Cabler’s license when connecting to a communication network.

Panduit Licensing

Only Panduit-certified cabling is authorized for Video Surveillance systems.

Tradesperson Licensing

A range of specific licenses is mandatory for tradespersons, including ACMA cabling, locksmithing, and security certifications.

Standards

Compliance with Australian Standards, including those listed in Appendix 5, is required. All devices must display the Regulatory Compliance Mark (RCM).

Notices of Deviation

Contractors must adhere to these standards when working on essential systems. Any deviations must be reported to the CSU Project Officer or Custodian. Work may only proceed following approval of the deviation.

2.6. Boom Gates

Boom gates installed at Charles Sturt must adhere to the following specifications to ensure functionality, durability, and integration with university security systems. Compliance with Australian Standards, particularly AS/NZS 3845, is mandatory.

Features and Specifications

- **Control Integration:**

  - Boom gates shall be controlled by the University network and security systems.
- **Vehicle Detection:**
  - In-ground vehicle detection loops must be installed to protect vehicles and allow seamless exit from the carpark.
- **Operation:**
  - Automatic powered operation is mandatory for all boom gates.
- **Construction:**
  - Boom gates shall be constructed of fiberglass or lightweight metal to ensure durability and ease of operation.
- **Networking and Security:**
  - Integration with the University network and security systems must comply with University Design Standards Section 13: Security.

Detailed Specifications

Boom gates at Charles Sturt University shall meet the following minimum requirements:

- **Housing:** Heavy gauge steel housing with a powder coated finish for robustness and weather resistance.
- **Boom Arm:** A folding aluminium arm that accommodates available space without obstructing vehicular access when in the open position.
- **Motor:** Direct coupling motor to the boom for efficient and reliable operation.
- **Access Control and Intercommunication:**
  - Simple interface connections to the Access Control System and Intercommunication System with remote control capability.
- **Vehicle Restriction:**
  - Provide physical restriction to the car park area to vehicles with a width of 0.5m or greater.
- **Operation and Safety:**
  - Open to the vertical position.
  - Equipped with separate momentary action type remote release buttons for opening.
  - Automatic opening of egress boom gates via in-ground detection loops for vehicles leaving the car park.
  - Manual override (mechanical operation) in case of system failure.
  - Prevention of closure on a vehicle under the boom; if partially closed, the boom gate shall return to the vertical position.

    - Automatic closure with timeout timer and photo optical obstruction sensor for safety.
    - Weatherproof and vandal-resistant construction.
- **Status Indicator:**
    - Incorporate up/down status indicator on the access control system to facilitate monitoring and maintenance.

Consultation and Tailoring

- The project specification must be tailored to the specific requirements of each installation job.
- Consultants are required to consult with the University Physical Security Manager to discuss project needs and ensure compliance with all specified standards and regulations.

This standard ensures that boom gates across Charles Sturt University campuses are designed and installed to uphold the highest safety and operational standards, integrating seamlessly with existing security infrastructure while providing reliable access control and protection for university premises and users.

2.7. Defects Liability Period

DLP Maintenance and Response

The Defects Liability Period (DLP) covers a twelve (12) month operational maintenance period, commencing from the date of practical completion and the final acceptance of commissioning tests for the Essential Systems. The system will be considered operational once testing, training, and monitoring begin, and practical completion is granted.

DLP Maintenance Check Frequency

Two maintenance checks must be conducted during the DLP:

- First Maintenance Check: To be carried out within the first 6 months.
- Second Maintenance Check: To be scheduled 1 month before the expiration of the DLP.

Maintenance checks must take place during normal office hours and in the presence of the nominated Campus Facilities Management (CFM) representative. Specific dates for these checks should be agreed upon with CFM at least 14 days in advance. All maintenance must be performed by appropriately qualified and licensed personnel. After each check, detailed test sheets documenting the devices checked and their status must be provided to CFM and the designated coordinator.

DLP Maintenance Check Requirements

- During the maintenance visits, the vendor will complete and document the following tasks:
- Perform all system checks using the system password or master code.
- Inspect all 240-volt power supplies connected to the system.
- Test the functionality of power supplies.
- Test system operation on battery power and record start and end battery voltages.

- Check the condition and operation of reed switches, Request-to-Exit (REX) devices, locks, tamper switches, card readers, etc.
- Inspect all panels and termination cabinet connections for corrosion, and clean if necessary.
- Inspect wiring and conduits for any signs of tampering or damage.
- Test all devices to ensure the integrity of circuits throughout their entire length.

Second Maintenance Check

- During the second maintenance check, vendors will:
- Provide short refresher training sessions for staff and security personnel as needed.
- Clean all devices, including card readers, door locks, electric strikes, code pads, manual call points (MCP), etc.
- Reprogram functions of the Essential Systems as requested by CFM and approved by the designated coordinator.

3. Supporting Documentation

These below lists are not all-inclusive and those associated with the project are responsible for identifying and complying with all standards relevant to the scope of works.

3.1. Supporting Legislation

National Construction Code of Australia (NCC) 2022 (Cth)

Telecommunications Act 1997 (Cth)

Telecommunications Cabling Provider Rules 2014 (Cth)

Telecommunications (Interception and Access) Act 1979 (Cth)

Broadcasting Services Act 1992 (Cth)

Radiocommunications Act 1992 (Cth)

Privacy and Personal Information Protection Act 1998 no 133 (NSW)

Privacy and Personal Information Protection Regulation 2019 (NSW)

Privacy Code of Practice (General) 2003 (NSW)

Security Industry Act 1997 (NSW)

Security Industry Regulation 2016 (NSW)

Workplace Surveillance Act 2005 (NSW)

Workplace Surveillance Regulation 2017 (NSW)

Crimes (Surveillance Devices) Act 2010 (ACT)

Crimes (Surveillance Devices) Regulation 2017 (ACT)

Information Privacy Act 2014 (ACT)

Information Privacy Regulation 2014 (ACT)

Security Industry Act 2003 (ACT)

Security Industry Regulation 2003 (ACT)

Workplace Privacy Act 2011 (ACT)

3.2. Supporting Standards

Standard Number	Standard Title
AS/NZS CISPR 14.1:2021	Electromagnetic compatibility — Requirements for household appliances, electric tools and similar apparatus, Part 1: Emission (CISPR 14-1:2020 (ED 7.0) MOD)
AS 1345:1995	Identification of the contents of pipes, conduits and ducts
AS 1367:2023	Coaxial cable and optical fibre systems for the RF distribution of digital television, radio and in-house analogue television signals in single and multiple dwelling installations
AS 1428.1:2021	Design for access and mobility, Part 1: General requirements for access - New building work
AS 1428.2:1992	Design for access and mobility, Part 2: Enhanced and additional requirements — Buildings and facilities
AS 1428.4.2:2018	Design for access and mobility, Part 4.2: Means to assist the orientation of people with vision impairment — Wayfinding signs

Standard Number	Standard Title
AS 1428.5:2021	Design for access and mobility, Part 5: Communication for people who are deaf or hearing impaired
AS 1670.1:2024	Fire detection, warning, control and intercom systems - System design, installation and commissioning, Part 1: Fire
AS 1670.3:2018 Amd 1:2021	Fire detection, warning, control and intercom systems, Part 3: System design, installation and commissioning
AS 1670.4:2018 Amd 1:2021	Fire detection, warning, control and intercom systems - System design, installation and commissioning, Part 4: Emergency warning and intercom systems
AS 1670.5:2016	Fire detection, warning, control and intercom systems — System design, installation and commissioning, Part 5: Special hazards systems
AS 1670.6:2023	Fire detection, warning, control and intercom systems — System design, installation and commissioning, Part 6: Smoke alarm systems
AS/NZS 2201.1:2007	Intruder alarm systems: Client's premises - Design, installation, commissioning and maintenance: Part 1 - Intruder alarm systems.
AS 2201.2:2022	Alarm and electronic security systems, Part 2: Monitoring centres
AS 2201.3-1991	Intruder alarm systems, Part 3: Detection devices for internal use
AS/NZS 2201.5:2008	Intruder alarm systems, Part 5: Alarm transmission systems
AS 1768:2021	Lightning protection
AS/NZS 3000:2018	Electrical installations (known as the Australian/New Zealand Wiring Rules)
AS/NZS 3845.1:2015	Road safety barrier systems and devices, Part 1: Road safety barrier systems
AS/NZS 3845.2:2017	Road safety barrier systems and devices, Part 2: Road safety devices
AS/NZS 4295:2015 Amd 1:2015	Part 3 – Analogue Speech (Angle Modulated) Equipment Standard
AS/NZS 4355:2006	Handphone equipment and HF CB radio equipment
AS/NZS 4365:2011	Part 7 – UHF CB Equipment Standard
AS 4607-1999	Personal response systems
AS/NZS 4770:2000 AMDT 1	MF and HF landphone mobile equipment
AS 4806.1:2006	Closed-circuit television (CCTV) systems for use in security applications: Part 1 - System design, commissioning and maintenance.
AS 4083:2010	Planning for emergencies - Health care facilities
AS 4933:2015	Digital television — Requirements for receivers for VHF/UHF DVB-T television broadcasts including ancillary services
AS/NZS 5000 Series	Electric cables - Polymeric insulated
AS 5007:2007	Powered doors for pedestrian access and egress
AS 60529:2004	Degrees of protection provided by enclosures (IP Code)
AS/NZS 61000 Series	Electromagnetic compatibility (EMC)
AS/NZS IEC 60079 Series	Explosive atmospheres
AS/NZS IEC 60839.11.1:2019	Alarm and electronic security systems, Part 11.1: Electronic access control systems — System and components requirements
AS/NZS IEC 60839.11.2:2019	Alarm and electronic security systems, Part 11.2: Electronic access control systems — Application guidelines
AS/NZS IEC 60839.11.31:2020	Alarm and electronic security systems, Part 11.31: Electronic access control systems — Core interoperability protocol based on Web services

Standard Number	Standard Title
AS 61386.1:2015	Conduit systems for cable management, Part 1: General requirements
AS/NZS 62676.1.1:2020	Video surveillance systems for use in security applications, Part 1.1: System requirements — General (IEC 62676-1-1:2013, MOD)
AS/NZS IEC 62676.2.31:2020	Video surveillance systems for use in security applications, Part 2.31: Live streaming and control based on web services
AS/NZS IEC 62676.3:2020	Video surveillance systems for use in security applications, Part 3: Analog and digital video interfaces
AS/NZS 62676.4:2020	Video surveillance systems for use in security applications, Part 4: Application guidelines (IEC 62676-4:2014, MOD)
AS/NZS 62676.5:2020	Video surveillance systems for use in security applications, Part 5: Data specifications and image quality performance for camera devices (IEC 62676-5:2018, MOD)
AS ISO 7240.18:2018	Fire detection and alarm systems, Part 18: Input/output devices
ETSI EN 300 224 V2.1.1 (2017-06)	Paging service equipment

3.3. Industry Codes of Practice

Protective Security Policy Framework

https://www.protectivesecurity.gov.au/

Australia Communications Authority Technical Standards

https://www.acma.gov.au/technical-standards

Australian Security Industry Association Limited (ASIAL): CCTV Code of Ethics

https://asial.com.au/Web/Web/Advice-Services/Standards-and-Codes/CCTV-Code-of-Ethics.aspx

3.4. Related University Policy

Facilities and Premises Policy

https://policy.csu.edu.au/document/view-current.php?id=465

Facilities and Premises Procedure - Access, Use and Security

https://policy.csu.edu.au/view.current.php?id=00239

Facilities and Premises Procedure - Corporate Signage

https://policy.csu.edu.au/document/view-current.php?id=193

Records Management Policy

https://policy.csu.edu.au/document/view-current.php?id=165

Surveillance Procedure

https://policy.csu.edu.au/document/view-current.php?id=499&version=1

3.5. Other Resources

Universities Australia Toolkit for Universities

https://universitiesaustralia.edu.au/policy-submissions/safety-wellbeing/toolkit-for-universities/