



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3036A Program security equipment and system

Release: 1

CPPSEC3036A Program security equipment and system

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to program a range of security equipment and systems. It requires the ability to accurately determine configuration parameters and program security equipment and systems to meet client requirements. This work applies in extra low voltage as defined through the Australian standards AS 2201 (1986) environments.

This unit may form part of the licensing requirements for persons responsible for programming security equipment and systems in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit

This unit of competency has application in those work roles involving the programming of security equipment and systems. Competency requires legal and operational knowledge applicable to relevant sectors of the security industry. The knowledge and skills described in this unit are to be applied within relevant legislative and organisational guidelines.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Not Applicable

Employability Skills Information

Employability skills This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element. Where <i>bold italicised</i> text is used, further information is detailed in the required skills and knowledge section and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
---	--

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1 Prepare for programming.	1.1 Applicable provisions of legislative and organisational requirements relevant to assignment instructions are identified and complied with. 1.2 Assignment instructions are obtained, reviewed and confirmed as required with relevant persons. 1.3 Security equipment and system to be configured and programmed is identified and confirmed. 1.4 Programming requirements and configuration parameters appropriate to the security equipment and system are confirmed and clarified as required. 1.5 Tools, equipment and materials needed to carry out the work are selected and checked for correct operation and safety. 1.6 Potential and existing risks and hazards in the work area are identified and controlled in accordance with Occupational Health and Safety (OHS) requirements and own role, competence and authority.
2 Program security equipment and system.	2.1 Personal protection equipment is selected and used in accordance with OHS requirements. 2.2 Security equipment and system is powered, programmed and configured in accordance with assignment instructions. 2.3 Correct operational procedures and compliance requirements are observed and followed in accordance with manufacturer's instructions. 2.4 Configuration of security equipment and system is tested and checked using approved procedures. 2.5 Required adjustments to programming instructions are determined and confirmed with relevant persons. 2.6 Safe workplace practices are applied throughout programming process in accordance with OHS requirements.
3 Complete programming activities.	3.1 Programmed security equipment and system is inspected to confirm operational effectiveness and conformance with assignment instructions. 3.2 Work area is restored to original condition, waste disposed of and tools and equipment cleaned and stored in accordance with organisational requirements. 3.3 Malfunctions, faults, wear or damage to tools or equipment is documented and reported for repair or replacement in accordance with organisational procedures.

ELEMENT**PERFORMANCE CRITERIA**

- 3.4 Notification of work completion is made to relevant persons in accordance with organisational procedures.
- 3.5 Relevant **documentation** is completed and securely maintained in accordance with organisational procedures.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge and their level required for this unit.

Required skills

- accurately identify and handle cables
- apply safe and environmentally aware work practices
- communicate in a clear and concise manner
- complete documentation
- download and upload digital information
- estimate and organise materials, tools and equipment requirements
- identify and comply with applicable legislative requirements including licensing
- identify and control workplace hazards
- identify and follow routine workplace safety procedures
- identify and report faulty equipment
- operate security equipment and systems
- organise and prioritise work tasks
- power security systems
- program and configure security equipment and systems
- read a multimeter
- read and interpret plans and specifications
- solve routine problems
- test security equipment and systems
- use suitable tools and equipment, including hand and power tools
- work in confined spaces.

Required knowledge

- applicable legislative requirements including licensing and client confidentiality
- building construction methods and types
- cable identification methods and techniques
- earthing systems arrangements and requirements
- electrical concepts

REQUIRED SKILLS AND KNOWLEDGE

- emergency procedures
- keypad and control panel types and functions
- methods of equipment and system programming
- procedures for accessing and storing tools, equipment and materials
- procedures for reporting malfunctioning or faulty tools and equipment
- procedures to power systems
- reporting and documentation requirements
- requirements for compliance with Australian building codes and regulations and Australian Communications Authority cabling standards
- requirements for working at height and in a confined space
- risks and hazards associated with programming procedures
- safe workplace procedures
- technical terminology
- types and functions of computer software
- types of security equipment and system configurations
- types, functions and features of security equipment and systems
- waste disposal procedures.

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

A person who demonstrates competency in this unit must be able to provide evidence of:

- interpreting and complying with all applicable legislative and licensing requirements for programming work
- accessing security equipment and systems with minimal disruption to client, services or normal work routines
- accurately determining programming requirements and configuration parameters of security equipment and systems
- applying appropriate methods to program and configure security equipment and systems
- cleaning and storing tools and equipment and reinstating work site to a clean and safe condition
- following safe and efficient work practices in the use of tools and equipment and managing risks and hazards in the work area

- organising own work tasks within specified programming timeframes and completing documentation related to programming services
- carrying out checks to ensure the integrity, security and safety of security equipment and system.

Context of and specific resources for assessment

Context of assessment includes:

- a setting in the workplace or environment that simulates the conditions of performance described in the elements, performance criteria and range statement.

Resource implications for assessment include:

- access to plain English version of relevant statutes and procedures
- access to a registered provider of assessment services
- access to a suitable venue and equipment
- assessment instruments including personal planner and assessment record book
- work schedules, organisational policies and duty statements.

Reasonable adjustments must be made to assessment processes where required for people with disabilities. This could include access to modified equipment and other physical resources, and the provision of appropriate assessment support.

Method of assessment

This unit of competency could be assessed using the following methods of assessment:

- observation of processes and procedures
- questioning of underpinning knowledge and skills.

Guidance information for assessment

Assessment processes and techniques must be culturally appropriate and suitable to the language, literacy and numeracy capacity of the candidate and the competency being assessed. In all cases where practical assessment is used, it should be combined with targeted questioning to assess the underpinning knowledge.

Oral questioning or written assessment may be used to assess underpinning knowledge. In assessment situations where the candidate is offered a choice between oral questioning and written assessment, questions are to be identical.

Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.

Range Statement

RANGE STATEMENT

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Legislative requirements may relate to:

- applicable commonwealth, state and territory legislation which affects work such as:
 - workplace safety
 - environmental issues
 - equal employment opportunity
 - industrial relations
 - anti-discrimination and diversity
- Australian building codes and regulations
- Australian Communications Authority cabling standards
- Australian standards and quality assurance requirements
- award and enterprise agreements
- evidence collection
- freedom of information
- licensing arrangements and certification requirements
- privacy requirements
- relevant industry codes of practice
- telecommunications
- trade practices.

Organisational requirements may relate to:

- access and equity policies, principles and practices
- business and performance plans
- client service standards
- code of conduct, code of ethics
- communication and reporting procedures
- complaint and dispute resolution procedures
- emergency and evacuation procedures
- employer and employee rights and responsibilities
- OHS policies, procedures and programs
- own role, responsibility and authority
- personal and professional development
- privacy and confidentiality of information
- quality assurance and continuous improvement processes and standards
- resource parameters and procedures
- roles, functions and responsibilities of security personnel

Assignment instructions may include:

- storage and disposal of information.
- access to site and specific site requirements
- equipment, tools and material requirements
- equipment and system location information
- personal protection clothing and equipment requirements
- reporting requirements
- security equipment and system information:
 - features, functions and capabilities
 - installation procedures
 - manufacturer's instructions
 - service and maintenance requirements
 - type
 - warranties and guarantees
- specific client requirements
- timeframes
- work schedules
- work tasks and procedures.

Relevant persons may include:

- clients
- colleagues
- engineers and technicians
- equipment and systems manufacturers
- security consultants
- security personnel
- site managers or project managers
- supervisor.

Security equipment and systems may include:

- access control systems
- audible and visual warning devices
- cameras and monitors
- commercial and residential alarm systems
- detection devices
- electric and mechanical fire safety and fire locking systems
- electronic locks and locking systems
- electronic readers
- electronic screen equipment
- intercoms and control panels
- security doors and door controls
- specialised access control systems eg biometrics.

Security systems may be:

- computerised
- electronic
- mechanical

Tools, equipment and materials may include:

- procedural.
- cable testing equipment
- communications equipment
- computer disks
- crimp tools
- hand tools
- ladder
- multimeter
- personal protection equipment
- power tools
- templates.

Risks and hazards may relate to:

- chemical hazards eg battery corrosion
- exposed electrical wiring
- exposure to:
 - asbestos
 - building debris
 - dust
 - glass fibre
 - live power
 - natural and other gas build-up
 - noise
 - vermin
 - water
- manual handling
- non-compliance with building codes and regulations.

Occupational Health and Safety (OHS) requirements may relate to:

- emergency procedures
- following confined spaces procedures
- implementation of safety policies and procedures
 - chemicals, gas and vapour
 - isolation procedures
 - monitoring and testing procedures
 - use of personal protection equipment and clothing
 - work clearance procedures
- risk and hazard recognition
- safety training
- working with electrical wiring and cables
- working with tools and equipment.

Personal protection equipment may include:

- breathing apparatus
- fire extinguisher
- first aid kit

- gloves
 - head protection
 - hearing protection
 - knee pads
 - masks
 - safety boots
 - safety glasses.
 - warning signs and tapes
 - witches hats.
- Documentation may include:**
- adjustments to original cable plan
 - faulty or malfunctioning tools and equipment
 - materials used
 - security equipment and system positioning
 - testing and inspection results
 - work activity report
 - written and electronic reports.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Technical security