



Australian Government

Department of Education, Employment and Workplace Relations

CSCSAS201A Maintain security

Revision Number: 3

CSCSAS201A Maintain security

Modification History

Release	TP Version	Comments
3	CSC12 V1.1	Editorial corrections to Range Statement
2	CSC12 V1	Layout adjusted. Minor revisions to required skills and range statement.
1	CSC07 V1.2	Primary release.

Unit Descriptor

This unit of competency describes the outcomes required to implement effectively and confidently the security policies of the organisation. It covers the competency to assess and respond to general security risks.

Application of the Unit

This unit is a core unit for all certificate qualifications and applies to all people working in detention centres, correctional centres or prisons, community corrections offices, justice administration offices and on work sites where detainees, prisoners or offenders are under statutory supervision. Candidates will not hold statutory responsibility and will be supervised in their work duties.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

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 range statement. Assessment of performance is to be consistent with the evidence guide.
---	---

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1 Follow security procedures	1.1 Identify follow all <i>security and emergency procedures relevant to own work role.</i> 1.2 Calculate level of <i>security risk</i> according to organisational guidelines and instructions. 1.3 Implement relevant security procedures according to organisational policies, code of practice and legislation. 1.4 Alert work group members and relevant personnel using <i>appropriate equipment and terminology for emergency warnings.</i> 1.5 Report potential breaches of security to appropriate authority. 1.6 Participate in the <i>routine review of security procedures and responses</i> according to own level of responsibility.
2 Maintain security of information	2.1 Maintain <i>up-to-date and accurate records</i> in a form accessible to authorised personnel. 2.2 Relay relevant information to authorised personnel on the movement and circumstances of offenders. 2.3 Respond to requests for information promptly and according to agreed procedures, ensuring information is accurate, relevant and complete. 2.4 Manage security files according to agreed procedures and effective work practices.

Required Skills and Knowledge

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

Required skills:

- complying with security procedures
- using equipment for the purpose and in the manner intended and authorised
- operating and checking routine activities and equipment for security factors
- identifying faults in security procedures and problems in equipment and practices
- giving advice to others about security
- responding to incidents and emergencies
- using information systems

Required knowledge:

- an awareness of all aspects of organisation's policies, objectives, principles, philosophy, strategic plans and procedures relevant to security
- environmental or sustainability legislation, regulations and codes of practice applicable to industry
- requirements for incident records and reports
- requirements for emergency evacuation
- use of equipment and safety procedures
- faults and potential problems and the requirements for reporting them
- risks and emergencies and the requirements for identifying and responding to them
- strategies for reducing and managing risk factors
- duty of care responsibilities and requirements

Evidence Guide

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

Overview of assessment	Evidence for assessment must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.
Critical aspects for assessment and evidence required to demonstrate competency in this unit	In addition to integrated demonstration of the elements and their related performance criteria, look for evidence that confirms: • the knowledge requirements of this unit • the skill requirements of this unit • application of employability skills as they relate to this unit • the application of security procedures followed in a range of contexts (two or more) over time
Context of and specific resources for assessment	Valid assessment of this unit requires: • access to a workplace environment or one that closely resembles normal work practice and replicates the range of security conditions likely to be encountered by an individual working alone and as part of a team • access to a range of communication equipment relevant to the workplace • access to emergency resources • copies of legislation, policies, procedures and guidelines relating to security in the organisation • access to appropriate learning and assessment support when required
Method of assessment	The following assessment methods are suggested: • observation of performance in routine workplace activities within a range of agreed responsibilities and in various work locations • written and/or oral questioning to assess knowledge and understanding • completion of workplace documents and reports produced as part of routine work activities • third-party reports from experienced practitioners • simulations conducted in training programs • completion of performance feedback from supervisors and colleagues

Guidance information for assessment	This unit should be assessed in conjunction with all other units with components of safety and security. The unit contains knowledge that may be assessed off the job, for example in a structured learning process, and performance outcomes that should be assessed ideally in the workplace in routine activities and in conjunction with other units with specific functional focus. Assessment methods should reflect workplace demands, and any identified special needs of the candidate, including language and literacy implications and cultural factors that may affect responses to the questions. In all cases where practical assessment is used it will be combined with targeted questioning to assess the underpinning knowledge.
--	--

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 in the performance criteria is detailed below. Add any 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.

<i>Security and emergency procedures</i> must include:	• all aspects of organisation's policies and procedures relevant to security relating to own work role • security guidelines • supervision, management and accountability for movements and activities of staff, offenders and members of the public • use and maintenance of general security equipment relevant to work roles and responsibilities • relevant legislation and statutory requirements governing work role in the justice system
<i>Security risks</i> include any emergency identified by an organisational risk analysis, which may include:	• bomb • building invasion/armed invasion • civil disorder • death - accidental, natural, homicide or suicide • deliberate self-harm • escapes • failure of utilities • fire • flood • hazardous substances incidents • hostage situations • medical emergencies • preservation of crime scene • physical violence or assault • severe weather or storm damage • threats or intimidation • unauthorised entry
<i>Appropriate equipment and terminology for emergency warnings</i> may include:	• personal duress alarms • audible or visual alarms • audible or vibrating pagers • communications technology, including radios • coded or uncoded public address announcements • screen or monitor alerts • home detention anklets • itemisers

	• Biometrics • Biometrics as entry systems
<i>Routine review of security procedures and responses</i> may include:	• briefings • debriefings • critical incident stress debriefing • emergency exercises or simulations • table or desktop exercises • local emergency procedure training sessions
<i>Up-to-date and accurate records</i> may be written, electronic or paper-based and may include:	• computer databases • daily logs • occurrences or movement logs • journal records • incident reports • standard organisational forms • maintenance schedules

Unit Sector(s)

Safety and security.

Competency field

Not applicable.