Australian Government

DEFCO401C Maintain security in a Defence communications and information systems environment

Release: 2

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

DEFCO401C Maintain security in a Defence communications and information systems environment

Modification History

Release	TP Version	Comments
2	DEF12V2	Layout adjusted. No changes to content.
1	DEF12V1	Primary release.

Unit Descriptor

This unit covers the competency required to maintain personnel, physical, communications and information systems security within the Defence communications and information systems workplace.

Application of the Unit

This unit was developed for communications and information systems operators working within Defence but is applicable to any individual in this field of work.

The maintenance of personnel, physical, communications and information systems security are a fundamental requirement of communications and information systems operators.

Typically operators work independently and as part of a team under direct and/or indirect supervision, use discretion and judgement, and take responsibility for the quality of their outputs. All activities are carried out in accordance with relevant organisational policies and procedures.

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 ***bold italicised*** text is used, further information is detailed in the Required Skills and Knowledge and/or the Range Statement. Assessment of performance is to be consistent with the Evidence Guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. **Maintain physical security**	1.1 ***Physical security*** is maintained to ensure the safeguarding of official matter in accordance with specific workplace and ***Defence security guidelines.*** 1.2 Breaches of physical security are reported to appropriate personnel.
2. **Maintain communications security**	2.1 Classified and sensitive material is protected as it is passed over ***communications paths*** by the correct use of Defence communications security ***procedures*** and guidelines. 2.2 Classified and cryptographic material is handled in accordance with specific workplace and Defence guidelines. 2.3 Security violations are documented and reported to appropriate personnel.
3. **Maintain information system security**	3.1 Information systems media, assets and data are ***protected*** in accordance with specific workplace and Defence information systems security guidelines. 3.2 Breaches of security are ***recorded and reported*** to appropriate personnel.
4. **Maintain personnel security**	4.1 ***Personnel security principles*** are applied to protect against the threat of subversion, sabotage and espionage. 4.2 Breaches of security are recorded and reported to appropriate personnel.

Required Skills and Knowledge

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

Required Skills

- apply circuit procedures
- correctly handle classified/COMSEC material
- encourage other team members
- follow directives
- muster publications page by page
- open/close combination/cipher locks
- perform routine/field/emergency destruction procedures
- participate in a team
- perform publication amendments
- provide timely and accurate reports

Required Knowledge

- circuit procedures
- combination and cipher lock operation
- cryptographic handling requirements
- information systems security practices
- publication amendment procedures
- reporting and recording procedures
- roles and responsibilities of team members
- routine/field/emergency destruction procedures
- rules pertaining to page by page mustering of publications
- security requirements for classified material
- special handling procedures
- techniques for supporting others

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.

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

Assessment must confirm the ability to:

Physical security:

- correctly handle classified and sensitive material
- control access to secure areas
- follow checks and muster procedures
- correctly maintain logs and registers
- follow destruction procedures
- report breaches in accordance with approved guidelines and procedures.

Communications security:

- correctly handle classified and sensitive material
- maintain circuit discipline
- employ electronic protection methods

Information systems security:

- follow information systems security practices
- account for media and assets
- maintain data integrity

Personnel security:

- apply need to know principle
- be aware of own responsibilities

Consistency in performance

Competency should be demonstrated over time to ensure the individual is assessed across a wide variety of situations within the workplace.

Context of and specific resources for assessment

Context of assessment

Competency should be assessed in the workplace or in a simulated workplace environment.

Specific resources for assessment

Access is required to:

- security reference material and documentation
- destruction procedures/orders
- Standard Operating Procedures

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.

Physical security may include:	• Checks and musters • Controlling of access • Destruction procedures • Maintenance of logs and registers • Reporting of breaches • Security of areas and containers • Security of documents, classified material and equipment
Defence security guidelines may include:	• Communications publications • Communications security publications • Defence security publications • Information systems publications • National and allied publications
Communications paths may include:	• Electronic • Radio • Verbal • Visual
Procedures may include:	• Allied procedures • National procedures • Service specific procedures • Workplace specific procedures
Protecting information systems may include:	• Accountability of computer assets • Application of information systems security and practices • Control of computer software • Integrity of data • Security of networks
Reporting and recording procedures may include:	• Accurately reporting any violation of security, by means of: • verbal reports • written reports • combination of verbal and written reports • Maintaining logs and registers • Reading and interpreting relevant guidelines and procedures
Personnel security principles may include:	• Individual awareness of responsibilities • Need to know principle

- Security clearance requirements

Unit Sector(s)

Not applicable.