



Australian Government

DEFCMM001 Maintain security in a Defence communications and information systems environment

Release: 2

DEFCMM001 Maintain security in a Defence communications and information systems environment

Modification History

Release 2. Modifications have been made to the Assessment Conditions.

Release 1. This unit was released in DEF Defence Training Package release 1.0 and meets the Standards for Training Packages.

This unit supersedes and is equivalent to DEFCO401C Maintain security in a Defence communications and information system environment.

- Unit code updated
- Content and formatting updated to comply with new standards
- All PC transitioned from passive to active voice

Application

This unit involves the skills and knowledge required to Maintain security in a Defence communications and information systems environment.

It includes the skills required to maintain personnel, physical, communications and information systems security within the Defence communications and information systems workplace.

This unit applies to communications and information systems operators working within Defence but may be relevant to others who work in this field.

The skills and knowledge described in this unit must be applied within the legislative, regulatory and policy environment in which they are carried out. Organisational policies and procedures must be consulted and adhered to.

Those undertaking this unit would work independently and as part of a team, under direct and/or indirect supervision within specific communications environments. They would use discretion and judgement, and take responsibility for the quality of their outputs while performing specific tasks in a range of sometimes unpredictable contexts.

No licensing, legislative or certification requirements apply to unit at the time of publication.

Pre-requisite Unit

Not applicable.

Competency Field

Communications

Unit Sector

Not applicable.

Elements and Performance Criteria

ELEMENTS	PERFORMANCE CRITERIA
Elements describe the essential outcomes.	Performance criteria describe the performance needed to demonstrate achievement of the element.
1 Maintain physical security	1.1 Maintain physical security to ensure the safeguarding of official matters 1.2 Report breaches of physical security to appropriate personnel
2 Maintain communications security	2.1 Protect classified and sensitive material as it is passed over communications paths 2.2 Handle classified and cryptographic material 2.3 Document and report security violations
3 Maintain information system security	3.1 Protect information systems media, assets and data 3.2 Record and report breaches of security
4 Maintain personnel security	4.1 Apply personnel security principles to protect against the threat of subversion, sabotage and espionage 4.2 Record and report breaches of security

Foundation Skills

Foundation skills essential to performance are explicit in the performance criteria of this unit of competency.

Range of Conditions

Range is restricted to essential operating conditions and any other variables essential to the work environment.

Non-essential conditions may be found in the Companion Volume Implementation Guide.

Unit Mapping Information

This unit supersedes and is equivalent to DEFCO401C Maintain security in a Defence communications and information system environment.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6bdbab1e-11ed-4bc9-9cba-9e1a55d4e4a9>

Assessment Requirements for DEFCMM001 Maintain security in a Defence communications and information systems environment

Modification History

Release 2. Modifications have been made to the Assessment Conditions.

Release 1. This unit was released in DEF Defence Training Package release 1.0 and meets the Standards for Training Packages.

This unit supersedes and is equivalent to DEFCO401C Maintain security in a Defence communications and information system environment.

- Unit code updated
- Content and formatting updated to comply with new standards
- All PC transitioned from passive to active voice

Performance Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria on at least one occasion and includes:

- applying circuit procedures
- handling classified/COMSEC material
- opening/closing combination/cipher locks
- performing routine/field/emergency destruction procedures
- performing publication amendments
- maintaining physical security:
 - handle classified and sensitive material
 - control access to secure areas
 - follow checks and muster procedures
 - maintain logs and registers
 - follow destruction procedures
 - report breaches in accordance with approved guidelines and procedures
- maintaining communications security:
 - handle classified and sensitive material
 - maintain circuit discipline
 - employ electronic protection methods
- maintaining information systems security:
 - follow information systems security practices
 - account for media and assets
 - maintain data integrity
- maintaining personnel security:

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

Knowledge Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria and include knowledge of:

- 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

Assessment Conditions

Assessors must hold credentials specified within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must satisfy the Principles of Assessment and Rules of Evidence and all regulatory requirements included within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must occur in workplace operational situations. Where this is not appropriate, assessment must occur in simulated workplace operational situations that reflect workplace conditions.

Assessment processes and techniques must be appropriate to the language, literacy and numeracy requirements of the work being performed and the needs of the candidate.

Resources for assessment must include access to:

- a range of relevant exercises, case studies and/or simulations
- acceptable means of simulation assessment
- applicable documentation, including workplace procedures, regulations, codes of practice and operation manuals
- relevant materials, tools, equipment and PPE currently used in industry.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6bdbab1e-11ed-4bc9-9cba-9e1a55d4e4a9>