



Australian Government

CPPSEC3108 Store, protect and dispose of security information

Release: 1

CPPSEC3108 Store, protect and dispose of security information

Modification History

Release 1.

Supersedes and is non-equivalent to CPPSEC3012A Store and protect information.

Significant changes made to the unit to reflect current industry needs. This version first released with CPP Property Services Training Package Version 7.0.

Application

This unit specifies the skills and knowledge required to store, protect and dispose of security information, including evidence that may be used in future judicial proceedings.

It includes:

- storing information for future retrieval using methods that preserve and maintain data integrity
- monitoring information movement and security
- disposing of security information using appropriate disposal methods and maintaining records to track information disposal.

It applies to people working independently or under limited supervision as members of a security team.

This unit may form part of the licensing requirements for people engaged in security operations in those states and territories where these are regulated activities.

Pre-requisite Unit

Nil

Unit Sector

Security operations

Elements and Performance Criteria

Elements describe the essential outcomes.	Performance criteria describe what needs to be done to demonstrate achievement of the element.
1. Collect, assess and record security information.	1.1 Review and apply workplace procedures and policies when storing, protecting and disposing of security information. 1.2 Collect security information and assess for accuracy and potential future use to meet client requirements. 1.3 Clarify legal rights and responsibilities and apply to work

	tasks when protecting, storing and disposing of security information to meet client requirements with relevant persons. 1.4 Use information technologies to label, register and record security information in accordance with workplace requirements.
2. Store security information for future retrieval.	2.1 Assess storage requirements and address factors that may impact on the safety of stored information in consultation with relevant persons. 2.2 Store security information using methods that are appropriate to the required storage timeframe, that preserve information integrity and condition, and that prevent loss. 2.3 Safely store security information for future analysis, dissemination and use in accordance with workplace requirements. 2.4 Establish and maintain continuity logs to monitor information movement and security.
3. Dispose of security information.	3.1 Verify authorisation, with relevant persons, to dispose of security information. 3.2 Assess type of security information and select appropriate disposal method. 3.3 Dispose of security information using legal disposal methods. 3.4 Complete and securely maintain records to track information disposal in accordance with workplace requirements.

Foundation Skills

This section describes the language, literacy, numeracy and employment skills essential to performance in this unit but not explicit in the performance criteria:

- language skills to use security industry approved terminology
- writing skills to label, register and record security information and continuity logs, using information technology and using concise and factual data
- reading skills to interpret:
 - procedures and policies that clarify legal rights and responsibilities
 - security information and evidence in a range of written, digital and diagrammatic or pictorial formats, such as film, photos, legal documents and text messages
- speaking and listening skills to:
 - use questions and active listening to clarify and discuss factors that may impact on the safety of stored information
 - use paraphrasing to check understanding when verifying authorisation to dispose of security information

- interpret information contained in audio files
- numeracy skills to interpret and calculate security data in numerical format
- problem solving skills to:
 - validate the accuracy of security information
 - assess potential future use of security information
 - select storage methods that are suitable for the preservation requirements of different types of security information
 - select information disposal methods
- technology skills to use a range of common information technologies to access, store, study, retrieve, transmit and manipulate data and information.

Unit Mapping Information

Supersedes and is non-equivalent to CPPSEC3012A Store and protect information.

Links

Companion volumes to this training package are available at the VETNet website -
<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>

Assessment Requirements for CPPSEC3108 Store, protect and dispose of security information

Modification History

Release 1.

Supersedes and is non-equivalent to CPPSEC3012A Store and protect information.

Significant changes made to the unit to reflect current industry needs. This version first released with CPP Property Services Training Package Version 7.0.

Performance Evidence

To demonstrate competency in this unit, a person must store, protect and dispose of security information for two different security assignments. For each assignment, the person must use information technology to collect, assess, record, store and successfully retrieve in its original condition the following types of security information:

- two audio files
- two digital images
- two hard copy documents
- two text messages
- two emails.

In doing this, the person must meet the performance criteria for this unit.

Knowledge Evidence

To be competent in this unit, a person must demonstrate knowledge of:

- standard operating procedures and workplace policies that ensure compliance with legislative and regulatory requirements when storing, protecting and disposing of security information:
 - anti-discrimination and diversity
 - duty of care
 - limits of own authority
 - privacy and surveillance
 - workplace health and safety (WHS)
- approved communication terminology used in the security industry
- basic research techniques that can be used to collect and assess security information
- different types and formats of security information and evidence that require storage and preservation and may be used in future judicial proceedings
- factors that may impact on the safety of stored security information
- interpret security information provided in different formats and contexts
- legal methods for disposing of different types of security information and evidence

- methods for complying with privacy and confidentiality regulations when collecting, storing and disposing of security information
- operational functions of a range of information technologies used to collect, store, record, retrieve and dispose of security information in a range of formats
- procedures for verifying authorisation to dispose of security information
- storage and preservation methods for a range of security information and evidence formats that:
 - are appropriate to the required storage timeframe
 - are suitable for the effective retention and preservation of information in original condition
 - prevent cross contamination
 - prevent damage
 - prevent interference or tampering
 - prevent theft
- techniques for establishing and maintaining continuity logs to monitor information movement and security
- techniques for validating the accuracy and reliability of security information.

Assessment Conditions

Assessors must satisfy the requirements for assessors contained in the Standards for Registered Training Organisations (RTOs). All individuals engaged by a licensed RTO for security licensing purposes must hold both a security trainer's licence (where such a licence exists within the relevant jurisdiction) and a security operative licence that authorises the security activities about which the individual is training/assessing. Regulators may impose other assessor conditions to meet jurisdictional assessment requirements.

Assessment of performance must be undertaken in an operational workplace environment or environment that reflects workplace conditions. Tasks are to be performed to the level of proficiency and within the time limits that would be expected in a workplace.

The assessment of performance evidence must be done by direct observation of the learner by an assessor, either by an assessor observing the learner physically or by an assessor observing the learner via audio and visual media.

Assessment of performance evidence is only valid where the learner has been assessed performing the role of a security officer.

Assessors are responsible for ensuring that the person demonstrating competency has access to:

- specifications of assessment tasks to store, protect and dispose of security information
- appropriate documents, materials, equipment and personal protective equipment (PPE) currently used in industry
- information technologies required to gather, organise and present security information and documentation
- standard operating procedures and workplace policies related to the security work role and which specify requirements for complying with industry legislation and regulations.

Links

Companion volumes to this training package are available at the VETNet website -
<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>