|  |  |
| --- | --- |
| **UNIT CODE** | CPPSEC3XXX |
| **UNIT TITLE** | Store, protect and dispose of security information |
| **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:   * interpreting and complying with workplace procedures and policies and legal rights and responsibilities to collect, assess and record security information using a range of information technologies * storing information for future retrieval using methods that preserve and maintain data integrity * monitoring information movement and security * disposing of security information and evidence by verifying the authorisation for disposal, assessing the type of information, selecting appropriate disposal methods, and maintaining records to track disposal of information   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. |
| **PREREQUISITE UNIT** | Nil |
| **ELEMENTS** | **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 Interpret and comply with workplace procedures and policies for 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 when protecting, storing and disposing of security information to meet client requirements.  1.4 Use information technologies to label, register and record security information. |
| 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.  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. |
| ***FOUNDATION SKILLS***  A person demonstrating competency in this unit must have the following language, literacy, numeracy and employment skills:   * 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 * self-management skills to plan tasks to meet work timeframes * 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 equivalent to CPPSEC3012A Store and protect information |
| **LINKS** | Companion volumes to this training package are available at the VETNet website:  <https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b> |

|  |  |  |
| --- | --- | --- |
| **TITLE** | | CPPSEC3XXX Store, protect and dispose of security information |
| **PERFORMANCE EVIDENCE** | | |
| A person who demonstrates competency in this unit must store, protect and dispose of security information for two (2) 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 (2) audio files * two (2) digital images * two (2) hard copy documents * two (2) text messages * two (2) 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 including:   + 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 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.  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.  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 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.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b> | |

For inclusion in separate Companion Volume: Range Statements

|  |  |
| --- | --- |
| ***Workplace policies and legal rights and responsibilities*** may relate to: | * access and equity policies, principles and practices * client service standards * code of conduct and ethics * communication and reporting procedures * duty of care * employer and employee rights and responsibilities * licensing requirements * own role, responsibilities and authority * privacy and confidentiality of information * professional standards, code of conduct and ethics * resource parameters and procedures for accessing resources * risk management * storage and disposal of confidential information * workplace health and safety (WHS) policies and procedures |
| ***Security information*** may include: | * audio recordings * charts * computer-based information * data * drawings * evidence * logs * original and backup tapes * original, copy and negative film and photographs * photographs or images * physical items (eg specimens, samples) * radio or telephone records * reports * video recordings |
| ***Clients*** may include**:** | * corporations * members of the public * government agencies * insurance companies * judicial representatives * legal representatives * loss assessors * police representatives |
| ***Information technologies*** may include: | * computers * drones * facsimiles * mobile devices such as phones and iPads * printers * scanners * software |
| ***Factors*** that may impact on the safety of stored information may relate to: | * client requirements * commercial value of information * consequence of loss * cost of alternative arrangements * duration (eg short term or long term) * environmental considerations (eg temperature, humidity, light, electromagnetic fields) * intellectual property * legal requirements * potential to harm individuals, organisations and countries safety of information * potential use of information * principles for managing exhibits and evidence * requirements for retrieval * security (eg off organisational premises) * sensitivity of information |
| ***Relevant persons*** may include: | * clients * colleagues * information storage specialists * judicial representatives * police representatives * security personnel * supervisors |