



Australian Government

ICTPRG537 Implement security for applications

Release: 1

ICTPRG537 Implement security for applications

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Application

This unit describes the skills and knowledge required to implement security for software applications, including code access security, security access control, cryptographic and secure, input and output handling.

It applies to individuals who work as software developers, software engineers, system and security administrators and testers, and responsible for coding secure software applications.

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

Unit Sector

Programming and software development

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Implement policy-based code-access security	1.1 Identify purpose of application security in software development 1.2 Configure required platform security configuration files using security configuration tools 1.3 Define required restriction custom code access permission and restrict access to protected resources 1.4 Define required access restriction custom code access and run protected operations
2. Implement security access control	2.1 Plan and document authentication and authorisation strategy according to organisational policies and procedures 2.2 Develop and document required application authentication and authorisation strategy

ELEMENT	PERFORMANCE CRITERIA
3. Write encrypt and decrypt code data	3.1 Determine and document required standard cryptographic algorithms 3.2 Encrypt, and decrypt, data using standard cryptographic algorithms
4. Protect application against injections	4.1 Plan and document secure input and output handling and prevent vulnerabilities related to code injections 4.2 Use secure input and output handling according to task requirements

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

SKILL	DESCRIPTION
Oral communication	Articulates requirements and responsibilities distinctively, using effective communication techniques and industry standard technical language intended for audience and environment
Reading	Evaluates complex and varied information, and concepts, in software security
Writing	- Prepares technical workplace documents detailing processes and outcomes that fulfil the expectations of different stakeholders - Writes and edits computer code, and technical data using correct syntax and logical flow
Planning and organising	- Takes responsibility for planning, sequencing and prioritising processes and tasks to achieve the required outcomes - Uses a range of digital tools and sophisticated techniques to meet desired outcomes - Is acutely aware of the importance of data security and of monitoring, and controlling, access to digitally stored and transmitted information
Problem solving	- Uses nuanced knowledge of context to demonstrate knowledge of anomalies and subtle deviations to normal expectations, focusing attention and remedying problems as they arise - Applies systematic and analytical problem-solving processes, in order to develop required security access control strategies
Technology	Demonstrates knowledge of principles, concepts, language and practices associated with the digital world

Unit Mapping Information

Supersedes and is equivalent to ICTPRG507 Implement security for applications.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTPRG537 Implement security for applications

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- secure at least two different applications.

In the course of the above, the candidate must:

- plan a security strategy
- prevent security attacks
- document processes and outcomes.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- industry standard hardware and networking relating to implementing security for applications
- industry standard programming algorithms and object-oriented programming used to implement applications security
- mathematics required for programming algorithms.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- security configuration tools required to implement security for applications
- required software development environment
- testing and debugging tools applicable to implementing security for applications
- network resources required to implement security for applications.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>