



Australian Government

ICTPRG507 Implement security for applications

Release: 1

ICTPRG507 Implement security for applications

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

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 may be responsible for coding secure software applications and who may work as software developers, software engineers, system and security administrators, and testers.

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 in an application	1.1 Identify the purpose of application security in software development 1.2 Configure the platform security configuration files using security configuration tools 1.3 Define a custom code access permission, to restrict access to protected resources or to run protected operations
2. Implement security access control in an application	2.1 Plan an authentication and authorisation strategy 2.2 Develop an appropriate authentication and authorisation

ELEMENT	PERFORMANCE CRITERIA
	strategy for an application
3. Write code to encrypt and decrypt data for secure communication	3.1 Analyse the standard cryptographic algorithms 3.2 Encrypt, and decrypt, data using standard cryptographic algorithms
4. Protect an application against injections	4.1 Plan secure input and output handling, to prevent vulnerabilities related to code injections 4.2 Use secure input and output handling

Foundation Skills

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

Skill	Performance Criteria	Description
Reading	1.1, 3.1	Evaluates complex and varied information, and concepts, in software security
Writing	1.2, 3.2, 4.2	Writes and edits computer code, and technical data, ensuring the correct syntax and accuracy
Get the work done	1.2, 1.3, 2.1, 2.2, 3.2, 3.1, 4.1, 4.2	- Takes responsibility for planning, sequencing and prioritising processes and tasks to achieve the required outcomes - Applies systematic and analytical problem-solving processes, in order to develop appropriate security access control strategies - 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

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTPRG507 Implement security for applications	ICAPRG507A Implement security for applications	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

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

Assessment Requirements for ICTPRG507 Implement security for applications

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the following must be provided:

- creating secure applications
- planning effective security strategies
- ensuring safe communications
- preventing security attacks.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

Evidence of the ability to:

- outline basic hardware, and networking
- outline basic programming algorithms
- explain object-oriented programming
- recognise the mathematics required for programming algorithms.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the programming and software development industry, and include access to:

- security configuration tools
- the software development environment
- testing and debugging tools
- the network resources
- the appropriate learning and assessment support, when required.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

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