



Australian Government

ICTNWK538 Install and maintain valid authentication processes

Release: 1

ICTNWK538 Install and maintain valid authentication processes

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 design, develop, install and maintain authentication processes and reduce vulnerability of a system.

It applies to individuals working in middle management roles including information security managers, network engineers, security analysts, or similar roles who are responsible for implementing and monitoring an organisational security management system.

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

Unit Sector

Networking

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. Evaluate authentication requirements	1.1 Determine user and organisational security requirements according to organisational security plan 1.2 Identify and analyse authentication options according to user and organisational requirements 1.3 Determine required authentication and authorisation processes according to organisational policies and procedures
2. Configure authentication system	2.1 Create required authentication realm and reuse according to authentication system and organisational requirements 2.2 Add required users and authorisation rules to new realm according to authentication system requirements 2.3 Determine user attributes and user attribute set-up according to authentication system requirements

ELEMENT	PERFORMANCE CRITERIA
	2.4 Set up authentication filter and authorisation parameters according to authentication system requirements
3. Apply authentication methods	3.1 Develop and document authentication systems and protocols according to authentication system requirements 3.2 Develop, document and distribute user authentication system responsibilities to required personnel 3.3 Apply authentication system to network and user according to system product and authentication system requirements 3.4 Record and securely store permission and configuration information according to authentication system requirements
4. Monitor authentication system	4.1 Review authentication system according to user security and quality of service requirements 4.2 Determine and document security monitoring, incident management and reporting processes according to organisational security plan 4.3 Submit documentation and respond to feedback from to required personnel 4.4 Seek and respond to feedback from required personnel according to organisational policies and procedures

Foundation Skills

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

SKILL	DESCRIPTION
Reading	Interprets and analyses technical data to determine requirements according to user and organisational plans
Writing	Prepares documentation detailing work performed according to organisational policies and procedures for a specific audience
Planning and organising	Uses a combination of formal, logical planning processes and an increasingly intuitive knowledge of context to plan control methods and systems processes
Problem solving	- Demonstrates a high-level knowledge of ways in which digital systems and tools are used or could be used to achieve work goals and begins to recognise strategic and operational applications - Uses intuition to identify authentication failure and security incidents and their general problem area - Demonstrates an analytical thought processes to clarify goals and key issues and lateral thinking processes to generate possible solutions

SKILL	DESCRIPTION
Self-management	- Follows explicit and implicit protocols and meets expectations associated with own role - Uses digital technologies and systems safely and securely when implementing and monitoring a system with a growing awareness of the permanence and transparency of all activities

Unit Mapping Information

Supersedes and is equivalent to ICTNWK503 Install and maintain valid authentication processes.

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 ICTNWK538 Install and maintain valid authentication processes

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:

- design and deploy authentications solutions to a medium-sized business technology environment.

In the course of the above, the candidate must:

- configure authentication software and tools
- align authentication processes to organisational requirements and industry standard best practices
- document work plans and processes.

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:

- problems and challenges associated with organisational authentication issues, including resource accounting through authentication
- industry standard virtual private network (VPN) issues, including:
 - quality of service (QoS) considerations
 - bandwidth
 - dynamic security environment
 - function and operation of VPN concepts
- authentication adaptors, including biometric authentication adaptors
- digital certificates, including:
 - VeriSign
 - X.509
 - SSL

- function and operation of authentication controls and protocols including:
 - passwords and personal identification numbers (PINs)
 - smart cards biometric devices
- network authentication services including:
 - Kerberos
 - NT LAN Manager (NTLM)
- features of common password protocols, including:
 - challenge handshake authentication protocol (CHAP)
 - challenge phrases
 - password authentication protocol (PAP)
 - remote authentication dial-in user service (RADIUS) authentication
- principles of security tokens.

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.

- a site or prototype where network authentication may be implemented and managed
- network support tools currently used in industry
- organisational security policies related to authentication
- manufacturers recommendations
- current authentication standards, including biometric authentication adaptors.

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>