



Australian Government

ICTNWK406 Install, configure and test network security

Release: 1

ICTNWK406 Install, configure and test network security

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 install, configure and test network security in an information and communications technology (ICT) network.

It applies to individuals working as ICT professionals who install, configure and test secure networks of any size.

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. Assess network security threats and vulnerabilities to identify risk	1.1 Assess and report on current system security, according to required asset security level 1.2 Determine additional network, software, hardware and system security threats and vulnerabilities 1.3 Use identified threats and vulnerability information to identify security risks 1.4 Make recommendations to management to address security deficiencies, according to current and future commercial and business requirements
2. Implement countermeasures for identified vulnerabilities	2.1 Implement required level of perimeter security based on current and future business needs

ELEMENT	PERFORMANCE CRITERIA
and threats	2.2 Assess and implement best practice server and network hardening techniques and measures 2.3 Implement secure authentication and user account controls 2.4 Secure data integrity and transmission
3. Test and verify functionality and performance of security system implemented	3.1 Design test items to verify key function and performance measures against criteria 3.2 Conduct function and performance tests recording results 3.3 Modify and debug security system as necessary 3.4 Develop documentation on current system settings and file for future reference
4. Provide systems for monitoring and maintaining security	4.1 Monitor current network security, including physical aspects, using appropriate third party testing software where applicable 4.2 Review logs and audit reports to identify and record security incidents, intrusions or attempts 4.3 Carry out spot checks and audits to ensure that procedures are not being bypassed 4.4 Document newly discovered security threats, vulnerabilities and risks in a report for presentation to appropriate person to gain approval for changes to be made

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	4.2	Recognises and interprets textual information to determine specific information about security incidents
Writing	1.1, 1.4, 3.2, 3.4, 4.4	Accurately records test results and develops material for a specific audience, using clear and detailed language in order to convey explicit information
Oral	1.1, 1.4, 4.4	Articulates information clearly, using specific and relevant language suitable to audience to convey

Communication		- recommendations and provide verbal reports - Uses listening and questioning techniques to confirm understanding
Numeracy	1.4	Extracts and evaluates the mathematical information embedded in a range of tasks and texts
Get the work done	1.1-1.4, 2.1, 2.3, 2.4, 3.1-3.3, 4.1, 4.3	- Determines job priorities, resources and equipment, and works logically and systematically to undertake clearly defined and familiar tasks - Understands the purposes, specific functions and key features of common digital systems and tools, and operates them effectively to complete routine tasks - Recognises and responds to predictable routine problems related to own role in the immediate work context, including detecting intrusion and debugging the system when required - Automatically implements standard procedures for routine decisions

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK406 Install, configure and test network security	ICANWK406A Install, configure and test network security	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 ICTNWK406 Install, configure and test network security

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 ability to:

- assess and identify security threats, vulnerabilities and risks
- determine appropriate countermeasure for threat, vulnerability or risk
- implement countermeasure per threat or risk
- install, configure and test network elements to ensure perimeter security
- test and verify function and performance of selected security measures
- monitor network for suspicious activity and take appropriate action where necessary
- document newly discovered threats, vulnerabilities and risks, including change recommendations for approval.

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

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- outline authentication issues
- summarise the security requirements of the client business domain, including:
 - organisation structure and business functionality
 - features and capabilities of networking technologies
 - privacy issues and privacy legislation
 - security information sources
 - risk analysis
- outline common virtual private network (VPN) issues, including bandwidth and dynamic security environment
- explain how to configure routers and switches
- summarise current industry accepted hardware and software security products, including general features and capabilities

- outline the function and operation of VPN concepts, including encryption, firewalls, packet tunnelling and authentication
- outline network protocols and operating systems
- summarise organisational issues surrounding security
- outline security perimeters and their functions
- describe security protocols, standards and data encryption
- summarise security threats, including eavesdropping, data interception, data corruption and data falsification
- outline types of VPNs, including site-to-site and user-to-site internet traffic and extranets
- summarise the systems and procedures related to:
 - audit and intrusion detection systems
 - auditing and penetration testing techniques
 - cryptography
 - local area network (LAN), wireless local area network (WLAN) and wide area network (WAN)
 - screened subnets
 - transmission control protocols or internet protocols (TCPs/IPs) and applications
 - use of virus detection software.

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 network industry, and include access to:

- a site where secure network installation may be conducted
- network security documentation
- equipment specifications
- network components
- hardware and software
- firewalls (hardware and software)
- a live network
- organisational guidelines
- networked (LAN) computers
- WAN service point of presence.

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>