



Australian Government

ICTNWK421 Install, configure and test network security

Release: 1

ICTNWK421 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 4.0.

Application

This unit describes the skills and knowledge required to install, configure and test network security in an organisational environment.

It applies to individuals who are involved in the installation, configuration, and testing of network security for networks of any size in job roles including network administrator, penetration tester, and security consultant.

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	1.1 Review current system security against organisational asset security requirements to identify security threats and vulnerabilities 1.2 Analyse network, software, hardware and system security threats and vulnerabilities to prioritise deficiencies to be addressed 1.3 Make recommendations to management to address security deficiencies according to organisational asset security requirements
2. Implement countermeasures for	2.1 Implement required level of perimeter security to meet organisational asset security requirements and according to

identified threats and vulnerabilities	identified threats and vulnerabilities 2.2 Assess and implement server and network hardening techniques and measures 2.3 Implement secure authentication and user account controls to secure data integrity and transmission
3. Test and verify functionality and performance of countermeasures implemented	3.1 Design function and performance test items to verify key functions and performance of countermeasures 3.2 Conduct function and performance tests to modify and debug countermeasures 3.3 Develop documentation on the current system settings and file according to organisational guidelines
4. Maintain and improve network security	4.1 Review logs and audit reports to identify and record security incidents, intrusions and attempts 4.2 Carry out spot checks and audits to ensure that procedures are not being bypassed 4.3 Document newly discovered security threats vulnerabilities and recommendations in a report for presentation to superior to gain approval recommendations to be implemented

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

Skill	Description
Reading	Recognises and interprets textual information to determine specific information about security incidents
Writing	Accurately records test results and develops material for a specific audience, using clear and detailed language in order to convey explicit information
Oral Communication	- Articulates information clearly, using specific and relevant language suitable to audience to convey recommendations and provide verbal reports - Uses listening and questioning techniques to confirm understanding
Numeracy	Extracts and evaluates the mathematical information embedded in tasks and texts
Get the work	Determines job priorities, resources and equipment, and works logically and systematically to undertake clearly defined and familiar

done	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
------	---

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK421 Install, configure and test network security	ICTNWK406 Install, configure and test network security	Edits to application to clarify intent and scope. Edits to elements 1–4 and assessment requirements to clarify intent. Edits to foundation skills to align with unit elements.	Equivalent unit

Links

Companion Volume Implementation Guides are available from VETNet -

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

Assessment Requirements for ICTNWK421 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 4.0.

Performance Evidence

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

- With respect to one network:
 - identify and analyse network security threats and vulnerabilities
 - make recommendations to management to address network security deficiencies and fulfil organisational asset security requirements
 - implement perimeter security, network hardening measures and authentication and user account controls according to identified deficiencies and organisational asset security requirements
 - design and conduct testing to verify the key function and performance measures of network security
 - debug network security according to test results
 - review logs and audit reports to identify and record five security incidents, intrusions and attempts
 - undertake three spot checks and audits to ensure that procedures are not being bypassed
-

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements and performance criteria of this unit. This includes:

- Security requirements of the organisation, including:
 - organisational structure and functions
 - features and capabilities of networking technologies
 - privacy issues and privacy legislation
 - security information sources
 - risk analysis

- Virtual private network (VPN) issues, including bandwidth and dynamic security environment
- Configuration of routers and switches
- Current hardware and software security products, including general features and capabilities
- Function and operation of VPN concepts including encryption, firewalls, packet tunnelling, and authentication
- Network protocols and operating systems
- Security perimeters and functions
- Security protocols, standards and data encryption
- Security threats including eavesdropping, data interception, data corruption and data falsification
- Types of VPNs including site-to-site and user-to-site internet traffic and extranets
- 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 protocol, internet protocol (TCPs/IPs), and applications
 - virus detection software

Assessment Conditions

Skills must be demonstrated in a workplace or simulated environment where conditions are typical of those in an ICT working environment or ICT workplace. This includes:

- Site where secure network installation, configuration, and monitoring may be conducted
- Network security documentation
- Organisational asset security requirements and information on organisational structure and functions
- Equipment specifications
- Network components
- Testing software
- Individual manager in the organisation
- Firewalls (hardware and software)
- Live network
- Networked (LAN) computers
- WAN service point of presence

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

Links

Companion Volume Implementation Guides are available from VETNet -

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