Australian Government

ICTNWK619 Plan, configure and test advanced server-based security

Release: 1

ICTNWK619 Plan, configure and test advanced server-based security

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 advanced server security using secure authentication and network services on a network server.

It applies to individuals working in network specialists roles, ICT network engineers, network security specialists, network security planners, network security designers.

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
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Plan advanced network server security	1.1 Determine required advanced network server environment 1.2 Analyse and review existing security documentation and identify network service vulnerabilities 1.3 Research required network authentication and network service configuration options and implications 1.4 Determine and document server security design solution according to organisational requirements
2. Prepare for network server security implementation	2.1 Assess environment and determine risk and hazard potential 2.2 Determine existing organisational risk and hazard

ELEMENT	PERFORMANCE CRITERIA
	control measures 2.3 Update existing risk control measures plan and align to installation requirements 2.4 Submit plan to required personnel, seek and respond to plan feedback 2.5 Implement risk and control preparation components according to technical and organisational requirements
3. Configure advanced network server security according to design	3.1 Configure required network authentication, authorisation, accounting services and automatic updates 3.2 Configure service security and access control lists according to technical design specifications 3.3 Configure required encryption and advanced network service security options 3.4 Configure operating system and third-party firewall and filter traffic in line with security requirements 3.5 Implement backup and recovery methods and enable restoration capability in the event of a disaster
4. Monitor and test network server security	4.1 Test and monitor server, server logs, network traffic and assess effectiveness of network service security 4.2 Monitor required files, detect unauthorised modifications, open ports and detect possible intrusions 4.3 Investigate, verify and document alleged violations of server and data security and privacy breaches 4.4 Implement required risk control measures plan recovery strategies and document outcomes 4.5 Finalise reports and documentation and submit to required personnel

Foundation Skills

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

SKILL	DESCRIPTION
Learning	• Considers the strategic and operational potential of digital trends to achieve work goals, enhance work processes, create opportunities and enhance or reduce risks

SKILL	DESCRIPTION
Oral communication	• Uses listening and questioning skills to confirm knowledge for requirements and when seeking and responding to feedback
Reading	• Interprets technical enterprise security procedures, policies, specifications and vendor notifications to determine and confirm job requirements
Writing	• Develops a broad range of material including security reports for a specific audience, using clear and detailed language to convey explicit information, requirements and recommendations
Teamwork	• Actively identifies the requirements of important communication exchanges, selecting required channels, format, tone and content to suit purpose and audience
Planning and organising	• Keeps up to date on changes to legislation or regulations required to own rights and responsibilities and considers implications of these when planning, negotiating and undertaking work
Problem solving	• Uses a broad range of strategies to store, access and organise virtual information, recognising that design choices will influence what information is retrieved and how it may be interpreted and used • Operates from a broad conceptual plan, developing the operational detail in stages, regularly reviewing priorities and performance during implementation and identifying and addressing issues
Self-management	• Uses nuanced knowledge of context to detect, investigate and recover from security breaches
Technology	• Demonstrates an acute awareness of the importance of knowledge, monitoring and controlling access to digitally stored and transmitted information

Unit Mapping Information

Supersedes and is equivalent to ICTNWK602 Plan, configure and test advanced server-based security.

Links

Companion Volume Implementation Guide is found on VETNet - https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2