Australian Government

ICTNWK403 Manage network and data integrity

Release: 1

ICTNWK403 Manage network and data integrity

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 lead the development of asset protection processes, determining threats and implementing controls to mitigate risk.

It applies to individuals working as middle managers including information security managers, network engineers and network technicians who are responsible for implementing and managing the organisational disaster recovery and asset protection policy and procedures.

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. Ensure compliance with company network and security policies	1.1 Review company security policies 1.2 Audit and record security access 1.3 Ensure user accounts are controlled 1.4 Ensure secure file and resource access
2. Conduct audit on system assets	2.1 Use appropriate tools and techniques to conduct audit on system hardware and software assets 2.2 Develop a system to record assets 2.3 Use system to develop reports on assets for management
3. Implement an antivirus	3.1 Research appropriate antivirus and anti-malware solutions

ELEMENT	PERFORMANCE CRITERIA
solution	3.2 Implement antivirus or anti-malware solution 3.3 Test antivirus and anti-malware solution functionality
4. Implement systems to protect assets from threats	4.1 Determine environmental threats to data 4.2 Document systems to protect from environmental threat 4.3 Implement system to protect data from environmental threat
5. Develop a backup solution	5.1 Determine appropriate backup type to meet systems needs 5.2 Investigate current backup media options 5.3 Implement a backup solution 5.4 Demonstrate functionality of backup solution 5.5 Demonstrate restore of data from backup media 5.6 Implement a real time backup and data sync solution
6. Monitor network performance	6.1 Determine available network performance monitoring tools 6.2 Implement network performance monitoring tools to monitor network 6.3 Produce report on network performance

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	• Interprets textual information from relevant sources to identify software solutions and adherence to company security policies
Writing	1.2, 2.2, 2.3, 4.2, 6.3	• Develops material for a specific audience, using clear and detailed language in order to convey explicit information, requirements and recommendations
Navigate the world of work	1.1	• Complies with explicit organisational policies and procedures
Get the work	1.2, 1.3, 2.1-2.3, 3.2,	• Determines job priorities, resources and equipment,

done	3.3, 4.1, 4.3, 5.1-5.6, 6.1, 6.2	and works logically and systematically to undertake clearly defined and familiar tasks • Takes responsibility for routine decision making by selecting from a range of predetermined options in routine situations, identifying and taking some situational factors into account • Initiates standard procedures when applying solutions in networks, including systems management processes, and deploys rapid solutions to problems involving management of network assets • Understands the purposes, specific functions and key features of common digital systems and tools, and operates them effectively to complete routine tasks • Understands the importance of secure information and privacy, and takes personal responsibility for identifying and managing risk factors

Range of Conditions

This section specifies different work environments and conditions that may affect performance. Essential operating conditions that may be present (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) are included.

Security policies must include:	• data security • physical security • remote access • user logon.

Tools must include:	• hardware and software audit tools, including:
	  • MSINFO32
	  • DXdiag
	  • Microsoft Software Inventory Analyzer (MSIA)
	  • E-Z Audit
	• hardware and software logs.

Backup type must include:	• copy • differential • folder and drive synchronisation • full and normal incremental • redundant array of independent disks (RAID).

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK403 Manage network and data integrity	ICANWK403A Manage network and data integrity	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet - https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2