Australian Government

ICTNWK547 Manage system security on operational systems

Release: 1

ICTNWK547 Manage system security on operational systems

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 and manage security on an operational system.

It applies to individuals working in middle management or leadership roles and are responsible for implementing and managing the organisations 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
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Analyse threats to system	1.1 Evaluate network security system and determine the level of alignment to organisational requirements 1.2 Conduct risk analysis on network security system and document outcomes 1.3 Identify and evaluate system threats and document findings according to organisational requirements 1.4 Identify and document system user interactions
2. Determine risk category	2.1 Conduct risk assessment on network security system and categorise risks 2.2 Conduct risk assessment on human operations and interactions with network security system and categorise risks 2.3 Match risk plans to risk categories according to risk

ELEMENT	PERFORMANCE CRITERIA
	assessment levels
	2.4 Determine and plan resources by risk categories according to risk assessment levels
3. Identify required controls	3.1 Devise and implement risk management controls according to system security requirements
	3.2 Plan and document required system-related user policies and procedures
	3.3 Identify high-risk categories at specified periods according to risk assessment levels
	3.4 Categorise and record system breakdowns according to organisational requirements
4. Implement controls in the system	4.1 Develop a management system security plan according to risk assessment levels and system security requirements
	4.2 Develop security recovery plan according to risk assessment levels and system security requirements
	4.3 Implement system controls and reduce risks in human interaction with the system
5. Monitor system tools and procedures	5.1 Conduct a management review process and monitor risks
	5.2 Review risk analysis process against security vendor benchmarks, security specialists and organisational requirements
	5.3 Determine and document re-evaluation system to identify new threats and risks
	5.4 Submit all documentation to required personnel, and seek and respond to feedback

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	• Demonstrates an increasing capacity to manipulate oral, visual and or written formats to achieve a specific purpose with full command of vocabulary required to context
Reading	• Gathers, interprets and analyses technical and enterprise information to determine requirements according to client needs
Writing	• Prepares information that incorporates a synthesis of knowledge, using Information and Communications Technology (ICT) terminology and cohesive language in a format and style required to a

SKILL	DESCRIPTION
	specific audience
Teamwork	• Recognises and addresses complex problems involving participation in group solutions and analysis and resolving issues for a mixed mode environment of people and systems processes
Planning and organising	• Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes • Uses a combination of formal and logical planning processes and an increasingly intuitive knowledge of context to develop a security plan and a security recovery plan
Problem solving	• Identifies and applies complex principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks • Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account
Self-management	• Takes full responsibility for identifying and considering required policies and procedures when managing a security system • Monitors and controls access to digitally stored and transmitted information

Unit Mapping Information

Supersedes and is equivalent to ICTNWK513 Manage system security.

Links

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