



Australian Government

ICTSAS440 Monitor and administer security of ICT systems

Release: 1

ICTSAS440 Monitor and administer security of ICT 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 monitor security functions of an Information and Communications Technology (ICT) system and administer security measures.

It applies to experienced individuals who, while working under a level of supervision, have responsibility in a frontline technical support capacity to ensure organisational standards are met and apply technical and specialised knowledge to maintain the security of an ICT system.

No licensing, legislative, or certification requirements apply to this unit at the time of publication.

Unit Sector

Systems administration and support

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. Access and control user accounts	1.1 Access ICT system according to organisational procedures 1.2 Modify default and previously created user settings according to security policies 1.3 Access and review logs and audit reports and identify security threats 1.4 Check the requirements for displayed legal notices at log on are aligned to organisational requirements 1.5 Check strength of passwords using required utilities 1.6 Review organisational guidelines for password complexity and tighten if required 1.7 Review password guidelines within other internal departments

ELEMENT	PERFORMANCE CRITERIA
	1.8 Check for and control legislation compliance breaches 1.9 Identify and resolve ICT system security
2. Secure file and resource access	2.1 Review inbuilt security features of file and resource access 2.2 Review and develop file security categorisation scheme 2.3 Monitor and record security threats to ICT system 2.4 Implement file and resource virus checking process 2.5 Schedule ICT system components virus checking process 2.6 Investigate and implement inbuilt and additional encryption facilities
3. Recommend and administer security measures	3.1 Perform user spot checks according to organisational policies and procedures 3.2 Document areas and instances where security procedures are not being followed 3.3 Create security adherence recommendations 3.4 Prepare and present audit report and recommendations to required personnel 3.5 Obtain recommended changes approval 3.6 Implement approved changes
4. Finalise ICT system security procedures	4.1 Conform all ICT system security checks have been performed 4.2 Review implemented security changes 4.3 Evaluate and report on system security procedures

Foundation Skills

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

SKILL	DESCRIPTION
Reading	Researches and analyses technical and non-technical information and system data from a range of sources to determine requirements and complete required actions
Writing	Prepares complex workplace documentation detailing information, requirements and recommendations using appropriate structure, layout and technical programming language
Oral Communication	Obtains information by listening and questioning and participates in verbal exchanges with a range of personnel using detailed and clear language to contribute information and

	express requirements and recommendations
Numeracy	• Uses mathematical equations to calculate and compare system and numerical data to determine required actions and prepare reports and schedules
Teamwork	• Selects and uses required conventions and protocols when communicating with others in a range of work contexts
Problem solving	• Applies analytical processes to resolve technical or conceptual problems
Self-management	• Takes responsibility for planning, sequencing and prioritising tasks and own workload for efficiency and effective outcomes
Technology	• Uses main features and functions of digital tools to complete work tasks

Unit Mapping Information

Supersedes and is equivalent to ICTSAS418 Monitor and administer security of an ICT system.

Links

Companion Volume Implementation Guide is found on VETNet -

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

Assessment Requirements for ICTSAS440 Monitor and administer security of ICT systems

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

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

- monitor and administer security functions of at least two different ICT systems.

In the course of the above, the candidate must:

- access and modify user settings to satisfy security policies, including:
 - legal notices at logon
 - password strength
 - email and resource access
- review user accounts for security control
- identify security features in operating environment
- monitor threats to the network using:
 - review logs and audit reports
 - third-party diagnostic tools
 - implementation of virus checking process and schedule
 - preparation of an audit report and recommendations
 - security spot checks.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- industry accepted hardware and software products related to IT security
- privacy issues and legislation with regard to IT security
- risk analysis processes for system security
- role of users in setting security
- password strength guidelines

- security technology and systems technologies
- client business domains, including:
 - client organisation structure
 - business functionality.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- special purpose tools, equipment and materials required for the monitoring and administration of security functions of ICT systems
- industry software packages
- an environment with an existing security system in place
- security policy for security systems
- industry and organisational standards
- a live ICT system.

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

Links

Companion Volume Implementation Guide is found on VETNet -

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