



**Australian Government**

# **ICTSAS418 Monitor and administer security of an ICT system**

**Release: 1**

# ICTSAS418 Monitor and administer security of an ICT system

## 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 monitor and administer security functions of an information and communications technology (ICT) system.

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 a 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. Ensure user accounts are controlled           | <ul style="list-style-type: none"><li>1.1 Modify default user settings to ensure they conform to security policy</li><li>1.2 Modify previously created user settings to ensure they conform to updated security policy</li><li>1.3 Ensure legal notices displayed at logon are appropriate</li><li>1.4 Check strength of passwords using the appropriate utilities and consider tightening rules for password complexity</li><li>1.5 Take action to ensure password procedures are reviewed with appropriate other internal departments</li><li>1.6 Monitor email to uncover breaches in compliance with</li></ul> |

| ELEMENT                            | PERFORMANCE CRITERIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | legislation<br>1.7 Access information services to identify security gaps and take appropriate action using hardware and software or patches                                                                                                                                                                                                                                                                                                                                                            |
| 2. Secure file and resource access | 2.1 Review inbuilt security and access features of the operating system and consider need for further action<br>2.2 Develop or review the file security categorisation scheme, and develop an understanding of the role of users in setting security<br>2.3 Monitor and record security threats to the system<br>2.4 Implement a virus checking process and schedule for the server, computer and other system components<br>2.5 Investigate and implement inbuilt or additional encryption facilities |
| 3. Monitor threats to the network  | 3.1 Use third-party software or utilities to evaluate and report on system security<br>3.2 Review logs and audit reports to identify security threats<br>3.3 Carry out spot checks and other security strategies to ensure that procedures are being followed<br>3.4 Prepare and present an audit report and recommendations to appropriate person<br>3.5 Obtain approval for recommended changes to be made                                                                                           |

## 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 | 1.3, 1.6, 1.7, 2.1, 2.2, 2.5, 3.1, 3.5 | <ul style="list-style-type: none"><li>Researches and analyses technical and non-technical information and system data from a range of sources to determine requirements and complete necessary actions</li></ul>                                                                            |
| Writing | 1.5, 2.2, 2.3, 3.1, 3.4                | <ul style="list-style-type: none"><li>Accurately records information and system data using required format, terminology and conventions specific to requirements</li><li>Prepares reports using concise language and correct spelling and grammar to convey explicit information,</li></ul> |

|                      |                             |                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |                             | requirements and recommendations                                                                                                                                                                                                                                                                                                                  |
| Oral Communication   | 1.5, 3.1, 3.5               | <ul style="list-style-type: none"> <li>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</li> </ul>                                                                       |
| Numeracy             | 1.1, 1.2, 2.3-2.5, 3.1, 3.2 | <ul style="list-style-type: none"> <li>Uses mathematical equations to calculate and compare system and numerical data to determine required actions and prepare reports and schedules</li> </ul>                                                                                                                                                  |
| Interact with others | 1.5, 3.4, 3.5               | <ul style="list-style-type: none"> <li>Selects and uses appropriate conventions and protocols when communicating with others in a range of work contexts</li> </ul>                                                                                                                                                                               |
| Get the work done    | 1.1-1.7, 2.1-2.5, 3.1-3.4   | <ul style="list-style-type: none"> <li>Takes responsibility for planning, sequencing and prioritising tasks and own workload for efficiency and effective outcomes</li> <li>Applies analytical processes to resolve technical or conceptual problems</li> <li>Uses main features and functions of digital tools to complete work tasks</li> </ul> |

## Unit Mapping Information

| Code and title<br>current version                             | Code and title<br>previous version                            | Comments                                                                                           | Equivalence status |
|---------------------------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------|
| ICTSAS418<br>Monitor and administer security of an ICT system | ICASAS418A<br>Monitor and administer security of an IT system | <p>Updated to meet Standards for Training Packages.</p> <p>Minor edit to the competency title.</p> | Equivalent unit    |

## Links

Companion Volume implementation guides are found in VETNet -

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

# Assessment Requirements for ICTSAS418 Monitor and administer security of an ICT system

## Modification History

| Release   | Comments                                                                                                     |
|-----------|--------------------------------------------------------------------------------------------------------------|
| Release 1 | This version first released with ICT Information and Communications Technology Training Package Version 1.0. |

## Performance Evidence

Evidence of the ability to:

- review user accounts for their security control
- identify security features available in the operating environment
- monitor, document and administer security functions on the system
- monitor threats to the network using:
  - third-party diagnostic tools
  - implementation of virus checking process and schedule
  - preparation of an audit report and recommendations.

Note: Evidence must be provided for at least TWO systems or occasions.

## Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- describe the key features of current industry accepted hardware and software products related to IT security
- discuss privacy issues and legislation with regard to IT security
- explain the key components of risk analysis process for system security
- describe the key features of specific security technology and systems technologies
- analyse the client business domain, including client organisation structure and business functionality.

## Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the systems administration and support field of work and include access to:

- special purpose tools, equipment and materials
- industry software packages
- the security policy
- industry and organisational standards
- a live system.

Assessors must satisfy NVR/AQTF assessor requirements.

## **Links**

Companion Volume implementation guides are found in VETNet -

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