Australian Government

ICTSAS501 Develop, implement and evaluate an incident response plan

Release: 1

ICTSAS501 Develop, implement and evaluate an incident response plan

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 develop and implement an incident response plan. The results of the incident response plan must be evaluated if they affect the mission of the organisation.

It applies to individuals who apply high-level technical skills and specialised knowledge to provide broad support functions in maintaining network service.

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
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Develop the incident response program	1.1 Develop the incident management policy 1.2 Identify services the incident response team should provide 1.3 Create incident response plans according to security policy and organisational goals 1.4 Develop procedures for incident handling and reporting 1.5 Create incident response exercises and red-teaming activities 1.6 Develop specific processes for collecting and protecting forensic evidence during incident response

ELEMENT	PERFORMANCE CRITERIA
	1.7 Specify incident response staffing and training requirements 1.8 Establish the response program
2. Implement the incident response program	2.1 Apply response actions in reaction to security incidents according to established policy, plans and procedures 2.2 Respond to and report incidents 2.3 Assist in collecting, processing and preserving evidence according to requirements 2.4 Execute incident response plans 2.5 Execute red-teaming activities and incident response exercises 2.6 Ensure lessons learned from incidents are collected in a timely manner and are incorporated into review plans 2.7 Collect, analyse and report incident management measures
3. Evaluate the incident response program	3.1 Assess efficiency and effectiveness of incident response program activities and implement changes as required 3.2 Examine effectiveness of red teaming and incident response tests, training and exercises 3.3 Assess effectiveness of communication between incident response team and related internal and external organisations, implementing changes where appropriate 3.4 Identify and implement improvements based on assessments of effectiveness

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, 1.2	• Analyses textual information and data to determine necessary actions
Writing	1.1, 1.3, 1.4, 1.6-1.8, 2.2, 2.6, 2.7	• Uses clear and accurate language and documentation formats appropriate to the task
Oral Communication	1.7, 2.2	• Uses clear and accurate language to provide and obtain information relevant to the task

Numeracy	1.3, 2.7	• Accurately interprets, analyses and documents numerical and technical system data • Uses mathematical equations to calculate data for technical reports
Navigate the world of work	1.3, 1.4, 1.6, 2.1	• Works autonomously, making high-level decisions to achieve and improve organisational goals • Develops and implements strategies that ensure organisational policies, procedures and regulatory requirements are met • Monitors and reviews the organisations policies, procedures and adherence to legislative requirements in order to implement and manage change
Interact with others	1.7, 2.2, 3.3	• Uses a variety of relevant communication tools and strategies in building and maintaining effective working relationships • Influences and fosters a collaborative culture facilitating a sense of commitment and workplace cohesion • Understands diversity and seeks to integrate diversity into the work context for managing change, making decisions and achieving shared outcomes
Get the work done	1.1-1.6, 1.8, 2.1-2.4, 2.6, 2.7, 3.1-3.4	• Plans strategic priorities and outcomes within a flexible, efficient and effective context in a diverse environment exposed to competing demands • Gathers and analyses data and seeks feedback to improve plans and processes • Addresses complex problems involving multiple variables, using formal analytical, lateral thinking techniques, experience and knowledge to focus in on the root cause • Explores new and innovative ideas to develop and improve performance

Unit Mapping Information

Code and title current version	**Code and title previous version**	**Comments**	**Equivalence status**
ICTSAS501 Develop, implement	ICASAS501A Develop, implement and	Updated to meet Standards for	Equivalent unit

Code and title current version	Code and title previous version	Comments	Equivalence status
and evaluate an incident response plan	evaluate an incident response plan	Training Packages	

Links

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