Australian Government

ICTSAS524 Develop, implement and evaluate an incident response plan

Release: 1

ICTSAS524 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 6.0.

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 systems administration and support functions.

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. Prepare to develop an incident response plan	1.1 Identify and document organisational incident response plan requirements 1.2 Identify and document incident response team services according to organisational requirements 1.3 Identify incident response plan structure according to organisational requirements 1.4 Determine and document alignment of organisation's existing incident response plan against identified requirements 1.5 Submit documentation to required personnel, seek and respond to feedback
2. Develop the incident	2.1 Develop and document incident management policy according

ELEMENT	PERFORMANCE CRITERIA
response plan	to task requirements 2.2 Create incident response plans according to organisational requirements and security policies and procedures 2.3 Develop incident handling and reporting procedures 2.4 Create incident response exercises, red-teaming activities, staffing and training requirements 2.5 Develop procedure for collecting and protecting forensic evidence during incident response procedures according to organisational requirements 2.6 Establish and document incident the response plan
3. Implement the incident response plan	3.1 Apply response actions to reported security incident according to incident response plan and task requirements 3.2 Assist in collecting, processing and preserving evidence according to requirements 3.3 Execute incident response plans, red-teaming activities and incident response exercises 3.4 Document security incident response and actions according to task requirements 3.5 Collect, analyse and report incident management measures according to task requirements
4. Evaluate incident response plans	4.1 Assess and document efficiency and effectiveness of incident response plans activities 4.2 Examine and document effectiveness of red teaming and incident response tests, training and exercises 4.3 Assess effectiveness of communication between incident response team and required internal and external organisations 4.4 Determine and document response improvement activities 4.5 Submit documentation to required personnel and obtain final task sign off

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	• Monitors outcomes of decisions, considering results and identifying key concepts and principles that may be adaptable in the future

SKILL	DESCRIPTION
Numeracy	• Interprets, analyses and documents numerical and technical system data • Uses mathematical equations to calculate data for technical reports
Oral communication	• Uses listening and questioning techniques to confirm task requirements and relevant information using succinct language
Reading	• Analyses textual information and data to determine necessary actions
Writing	• Prepares required workplace documentation detailing processes and outcomes using cohesive language
Teamwork	• 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
Planning and organising	• Monitors and reviews the organisations policies, procedures and adherence to legislative requirements in order to implement and manage change
Self-management	• Works autonomously, making high-level decisions to achieve and improve organisational goals
Problem solving	• Develops and implements strategies that ensure organisational policies, procedures and regulatory requirements are met • Operates from a broad conceptual plan, developing the operational detail in stages, regularly reviewing priorities and performance during implementation, and identifying and addressing issues

Unit Mapping Information

Supersedes and is equivalent to ICTSAS501 Develop, implement and evaluate an incident response plan.

Links

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