Contribute to operational information security management activities

Overview

Operational security management is a collection of associated security activities that help to maintain the ongoing security posture of an organisation. It consists of the monitoring, maintenance and management of the security aspects of the IT estate, its people, and its processes.

This standard covers the competencies required to contribute to operational security management activities under supervision. This includes secure operational and service delivery consistent with security policies, standards and procedures, raising organisational security awareness, asset and change management, managing security issues.

Contribute to operational information security management activities

Performance criteria

You must be able to:

1. assist with monitoring the application of information security operating procedures in line with organisational standards
2. regularly update information regarding operational information security management, including security controls, software patches and software updates
3. maintain operational information security logs, records and documentation in accordance with organisational standards
4. plan information security control updates including software patches and updated releases in line with organisational standards
5. check that approved software patches and updates have been fully implemented across all information systems in a timely manner
6. take appropriate and timely action to report security issues in line with organisational procedures
7. identify when and how to seek advice and guidance from other individuals during information activities

Knowledge and understanding

You need to know and understand:

1. the processes, procedures, methods, tools and techniques relating to operational security management
2. where to source the policies and standards that are relevant to operational security management activities
3. where to find the approved list of software patches and software updates
4. how to interpret organisational information security policies and standards that apply to information systems operations and apply them
5. how to implement audits to check that approved software patches and software updates have been applied to all relevant information systems
6. what is meant by operational information security management
7. the importance of maintaining logs relating to operational information security management activities
8. what are the roles and responsibilities of the operational information security management functions within the organisation
9. the importance of the need to report and respond to security issues rapidly and effectively following organisational policies and standards
10. the need for information systems activities to be carried out in accordance with organisational information security standards

Contribute to operational information security management activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60531
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, operational security management