TECIS60332

Contribute to secure software development activities

Overview

Information security breaches can lead to critical situations such as disclosure of customer information, denial of service, and threats to the continuity of business operations. These can have significant financial consequences, but the real cost to the organisation could be the loss of customer trust and confidence. This may be irreparable and impossible to quantify in monetary terms.

Software can be designed, developed, and deployed with information security considerations 'built in'. This includes factoring in necessary information security controls that minimise the risk exposure and the impact to the organisation if exploited. The information security features used to support secure software development can include: defining and implementing secure development standards; following the information security architecture for software development; implementing appropriate test strategies; verifying that developed software meets its security criteria (requirements and/or policy, standards & procedures); specifying processes to maintain the required level of security of software through its lifecycle and managing a system or component through a formal information security assessment.

This standard covers the application of secure development standards and practices. It also includes embedding of preventative security measures into software development to reduce the risk of threats and vulnerabilities on information systems and ensuring that testing demonstrates that security requirements are met.

Performance criteria

You must be able to:

1. embed information security controls into software development in line with organisational secure software development standards and the information security architecture
2. design and code strong authentication protections in line with organisational standards
3. utilise secure HTTP headers to prevent potential attacks in web applications in line with organisational standards
4. review and incorporate information security requirements into software development projects
5. use and apply the approved tools and techniques for secure software development to line with organisational standards
6. use appropriate information security testing tools to test software applications and identify security defects in software, in line with organisational standards
7. resolve information security related software defects using secure coding techniques in line with organisational standards

Knowledge and understanding

You need to know and understand:

1. what is meant by secure software development
2. why security needs to be built into software and information systems solutions
3. the types of application can be susceptible to security weaknesses
4. how security controls can be implemented into software development to protect systems and information
5. the attack types and software vulnerabilities that a software developer may encounter and need to protect against
6. the common security controls available in secure software development to prevent security incidents and to mitigate risk
7. the role of security testing in verifying the integrity of software solutions during development
8. the tools and techniques that are required during secure development activities and how to apply them
9. how to source and review the information security requirements for an information system or software solution in development
10. the policies, internal/external standards and external certifications relating to information assurance that any particular solution needs to comply with
11. the fact that building security software solutions after the design and development phases is more expensive and time consuming

TECIS60332

Contribute to secure software development 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	TECIS60332
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, secure software development