TECIS600202

Protect against cyber security threats

Overview

This standard covers the competences needed for non-cyber security specialists to contribute towards the cyber security resilience of an organisation. This includes the ability to protect against cyber security threats by following organisational policies and procedures that document the cyber security controls to be utilised.

Effective cyber security resilience occurs when not only cyber security professionals, but also the wider workforce are aware of the threats and vulnerabilities that exist both within and outside of an organisation. This standard is for those who are not cyber security professionals, but who are required to adopt cyber resilience practices and procedures whilst undertaking their own specialised tasks or functions.

The underpinning knowledge required to meet this standard will provide an understanding of the cyber security controls, tools and techniques, in order to defend against threats.

Performance criteria

You must be able to:

1. locate and review organisational cyber security policies to comply with them in the workplace
2. identify the technical and administrative cyber security controls implemented by organisations to contribute to cyber security resilience
3. maintain anti-malware protection to protect computer systems and data in line with organisational requirements
4. identify fraudulent communication phishing attempts (including email, instant message, text message or telephone calls) and respond to them
5. comply with organisational identity and access control policies and procedures when accessing different computer systems to maintain data security
6. apply data encryption to secure sensitive data (at rest and in transit) in line with organisational standards
7. select strong, unique passwords and preserve their non-disclosure in line with organisational password policies and procedures
8. use all available factors to provide multifactor authentication in line with organisational password policies and procedures
9. maintain software versions in line with organisational policies and standards
10. identify and remove software that is no longer supported or required in line with organisational policies and procedures
11. follow organisational standards for secure use of all devices in the work environment to maintain systems security
12. follow secure usage guidelines for unsecured USB ports and CD drives to prevent malicious or accidental transfer of malware to organisational systems and unauthorised extraction of data
13. maintain up to date cyber security awareness training in line with organisational requirements

Knowledge and understanding

You need to know and understand:

1. the need for cyber security controls to protect privacy and the confidentiality, integrity and availability of data
2. your organisation's policies and procedures for cyber security
3. how vulnerabilities can be mitigated through administrative controls
4. the phishing risks that can arise from communications (including email, messaging and telephone)
5. the role of software identity and access controls to restrict admission of different levels of authorised users and to grant privileged operations
6. how physical and environmental controls reduce the risk posed by threats within the physical environment, including natural or environmental hazards and physical intrusion by unauthorised individuals
7. why the organisation's computer network infrastructure is secured with appropriate technologies and processes, including switches, firewalls, segregation of duties and segmentation of computer networks into smaller stronger partitions
8. the need to identify and secure physical communications assets such as cabling, unsecured USB ports and CD read drives
9. why passwords used across business and social domains should be discrete, strong and unique
10. the different types of multi factor authentication (MFA) that are used in access control systems
11. the systems and procedures for encrypting sensitive data both in transit and at rest
12. the importance of keeping software versions up to date in line with organisational policies
13. the need to retire software that is no longer supported or required by the organisation
14. the importance of applying security controls across all devices whether fixed, mobile or from outside the organisation
15. the need to keep up to date with training and to manage own learning whether prescribed by the organisation or self-directed

Protect against cyber security threats

Developed by	ODAG
Version Number	1
Date Approved	April 2020
Indicative Review Date	March 2023
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd
Original URN	TECIS600202
Relevant Occupations	ICT for users
Suite	IT(Cyber Security)
Keywords	Information security, cyber security