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 individuals whose main work role is not that of a cyber security professional i.e. those who follow, maintain and enhance 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. Identify organisational cyber security policies, where to locate them, and what they contain
2. Comply with organisational cyber security resilience policies, procedures and guidelines
3. Recognise the cyber security controls, tools and techniques that are adopted in order to contribute to organisational cyber security strategy
4. Maintain up to date anti-virus and malware protection to protect computer systems and data, in line with organisational requirements
5. Identify fraudulent email, instant message, text message or telephone calls that may be phishing attempts and be aware of how to respond to them
6. Comply with organisational identity and access control approaches when accessing systems and data
7. Carry out the organisational processes for data encryption relating to data both at rest, and in transit
8. Maintain up to date cyber security resilience awareness training in line with organisational requirements
9. Select strong passwords and preserve their non-disclosure in line with organisational password policies and procedures
10. Maintain software versions in line with organisational policies and standards
11. Identify and remove software that is no longer supported or required
12. Follow organisational requirements for secure use of external storage devices (e.g. USB, CD/DVD, portable hard drives, SD/flash cards) and external access points, in order to maintain systems security

Knowledge and understanding

You need to know and understand:

1. The principles and benefits of cyber security resilience
2. How cyber security resilience contributes to information security
3. The importance of physical access as well as logical access controls used to limit data access to authorised people
4. How vulnerabilities can be prevented (e.g. by ensuring software updates are always kept up-to-date, and not opening unknown attachments or links from e-mails)
5. The measures required to ensure that access to information and systems is authorised
6. The purpose of encryption in protecting sensitive data and how encryption can improve data security
7. The organisational process for encryption relating to information - both in transit and at rest - and how to apply them
8. That physical and environmental security controls reduce the risk posed by threats within the physical environment, including natural or environmental hazards, and physical intrusion by unauthorised individuals
9. The importance of patch management and keeping software versions up to date
10. The need to retire software that is no longer supported or required That the organisation's network infrastructure is secured with appropriate technologies and processes, such as switches, firewalls and segregation
11. The need to secure physical communications assets such as cabling The need for secure usage of external storage devices (e.g. USB, CD/DVD, portable hard drives, SD/flash cards) and external access points, in order to maintain systems security
12. That both internal and external facing systems such as web applications and databases are designed to be secure

Protect against cyber security threats

Developed by	ODAG
Version Number	1
Date Approved	March 2020
Indicative Review Date	March 2023
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd
Original URN	TECIS60022
Relevant Occupations	ICT for users
Suite	IT Users
Keywords	Information security, cyber security