TECIS600203

Respond to and recover from cyber security breaches

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 respond to and recover from cyber security attacks by following organisational policies and procedures for disaster recovery and business continuity.

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 needed in order to defend against threats.

Performance criteria

You must be able to:

1. identify unauthorised access, or attempted access, to a system that breaches the system's security policy to affect its confidentiality, integrity or availability
2. recognise the symptoms of a cyber security attack and how to escalate these in line with organisational procedures
3. carry out appropriate tasks and responses to a cyber security attack in line with defined responsibilities and organisational policies and procedures
4. recognise and report security breaches in a timely manner following organisational incident response management procedures
5. locate and review organisational incident response policies and procedures to comply with them in the workplace
6. follow disaster recovery (DR) and business continuity planning (BCP) organisational standards to confirm system and data integrity following a cyber security attack

Knowledge and understanding

You need to know and understand:

1. why the organisation's systems, computer networks and data are continually monitored and any identified anomalies and weaknesses should be acted upon
2. why the objective of cyber security resilience is to maintain the organisation's ability to deliver services and intended outcomes despite adverse cyber events
3. the consequences for employees and organisations of different types of attack
4. why digital services and data are designed to be resilient in the event of disaster and can be recovered within required timescales
5. the common symptoms of a cyber security breach to an employee including unexpected browser add-on or plug-in, webcam light on when not in use, unexpected system slowness or the fans coming on more frequently.
6. the importance of reporting cyber security incidents and suspicious activity in an organisation to authorised staff
7. the steps involved in responding to a cyber security attack
8. the organisational policies and procedures to enable the recovery or continuation of vital technology infrastructure, systems and data following a cyber security event (including natural or human induced disasters)
9. why disaster recovery is part of business continuity and should be invoked after a cyber security attack to ensure all critical business functions are operational
10. cyber resilience being the ability of a business computing system to recover quickly should it experience security breaches
11. the organisation's plans for disaster recovery (DR) and business continuity (BC) and how to implement them
12. the importance of backup and recovery in preparedness for recovery in line with business continuity planning
13. the defined roles and responsibilities of authorised staff and the wider workforce for quickly discovering an incident and effectively containing the damage, eradicating the threat, and restoring the integrity of affected network and systems

Respond to and recover from cyber security breaches

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	TECIS600203
Relevant Occupations	ICT for users
Suite	IT(Cyber Security)
Keywords	Information security, cyber security