Unit 4520-307 Security of ICT systems

Level:	**3**
Credit value:	**12**
UAN:	**D/500/7220**

Unit aim

The aim of this unit is to teach the learner some of the fundamentals surrounding the security of ICT systems. In order to do this the learner will learn to identify common types of security breaches. The learner will also learn to describe methods of protection for data and systems as well as applying some of the security measures they have learnt about.

Learning outcomes

There are **three** learning outcomes to this unit. The learner will:

1. Know the common types of security threat to an organisation, its IT system and its data, with relevant methods and procedures for protecting it
2. Be able to apply security measures
3. Be able to monitor security procedures

Guided learning hours

Although patterns of delivery are likely to vary considerably, it is recommended that **100** hours should be allocated for this unit.

Endorsement of the unit by a sector or other appropriate body

This unit is endorsed by e-skills UK.

How is this unit assessed?

Assessment is by a learner portfolio.

Unit 4520-307 Security of ICT systems

Assessment Criteria

Outcome 1 Know the common types of security threat to an organisation, its IT system and its data, with relevant methods and procedures for protecting it

The learner can:

1. Describe the common types of security breach that can affect the organisation, such as:
    - unauthorised use of a system without damage to data;
    - unauthorised removal or copying of data or code from a system;
    - damage to or destruction of physical system assets and environment
    - damage to or destruction of data or code inside or outside the system
    - preventing normal use of a system (eg denial of service attack)
    - cultural differences
2. Describe specified data protection methods:
    - system data security facilities;
    - surveillance and monitoring methods;
    - effects of system configuration on data protection
3. Describe specified methods of providing physical security for ICT systems
    - access control devices (eg locks, biometric controls, CCTV) and their configuration
    - limiting visibility of data (eg by positioning of monitors, using encryption)
    - shielding (eg cable screening, Faraday cages)
    - types and appropriate uses of access records and authorisations
    - how to allocate access authority
4. Describe relevant organisational security procedures

Outcome 2 Be able to apply security measures

The learner can:

1. Configure and apply specified security tools to identify and prevent breaches of security, such as:
    - internal system tools (eg passwords and permissions, malware scanning, firewall, VPN, authentication and encryption facilities)
    - external tools (eg access control devices)

Outcome 3 Be able to monitor security procedures

The learner can:

1. Assist in ensuring compliance with organisational security procedures, including:
    - participating in security audits
    - gathering and recording information on security
    - initiating suitable actions to deal with identified breaches of security