SFJCECZH6
Investigate and implement IT security

Overview

This unit is about your ability to investigate and identify sources of threat to IT systems and how you make recommendations on IT security procedures and counter measures.

There are three elements

1 Investigate and identify sources of threat to IT systems
2 Contribute towards recommendations on IT security procedures
3 Make recommendations on IT security counter measures

Target Group

This unit is aimed at members of staff who are involved in preventing e-crime.

SFJCECZH6

Investigate and implement IT security

Performance criteria

Investigate and identify sources of threat to IT systems

You must be able to:

P1 location of **IT system(s)** is established
P2 you contribute towards allocating value to **IT systems** within the organisation
P3 you contribute to the analysis and identification of threat to **IT systems**
P4 the **type of threat** is defined
P5 the probability of threat is graded
P6 level of risk to organisation is graded and prioritised
P7 potential target(s) are identified
P8 security report is produced and distributed to **appropriate persons(s)**

Contribute towards recommendations on IT security procedures

You must be able to:

P9 recommendations are made on **siting of IT systems**
P10 recommendations are made for virus checking procedures
P11 recommendations are made on **access** levels
P12 recommendations are made for implementation of restrictions to **access**
P13 all recommendations made are commensurate with own level of responsibility
P14 recommendations are recorded and submitted to **appropriate persons** for consideration

Make recommendations on IT security counter measures

You must be able to:

P15 recommendations are made on the frequency of line management monitoring checks
P16 recommendations are made on the installation of **access restrictions**
P17 recommendations are made on the frequency of systems audits
P18 all recommendations made are commensurate with own level of responsibility
P19 recommendations are recorded and submitted to **appropriate persons** for consideration

SFJCECZH6

Investigate and implement IT security

Knowledge and understanding

You need to know and understand:

K1 types of threat
K2 validity of threat
K3 likelihood of threat
K4 information dissemination policy and procedures of organisation
K5 perimeters of access
K6 use of dedicated areas
K7 restriction of `lone working'
K8 supervision of visitors
K9 user authentication
K10 enforced paths
K11 segregation of networks
K12 remote diagnostic port protection
K13 network connection controls
K14 network routing controls
K15 log on procedures
K16 organisational reporting procedures
K17 regulatory and legislative requirements
K18 data encryption
K19 message authentication
K20 operational software controls
K21 changing control procedures

SFJCECZH6

Investigate and implement IT security

Additional Information

Scope/range related to performance criteria

Investigate and identify sources of threat to IT systems

1. **IT systems**
   - 1.1. single
   - 1.2. multi site

2. **Appropriate persons**
   - 2.1. line manager or other higher authority
   - 2.2. IT manager
   - 2.3. security manager

3. **Type of threat**
   - 3.1. espionage
   - 3.2. terrorist
   - 3.3. sabotage
   - 3.4. subversive
   - 3.5. personal security

Contribute towards recommendations on IT security procedures

4. **Access**
   - 4.1. internal
   - 4.2. external

5. **IT systems**
   - 5.1. single
   - 5.2. multi site

6. **siting of systems**
   - 6.1. on-site
   - 6.2. remote

7. **Appropriate persons**
   - 7.1. line manager or other higher authority
   - 7.2. IT manager
   - 7.3. security manager

Make recommendations on IT security counter measures

8. **types of access restrictions**
   - 8.1. software
   - 8.2. hardware

8.3. personnel
8.4. external
8.5. internal

9. **Appropriate persons**
9.1. line manager or other higher authority
9.2. IT manager
9.3. security manager

SFJCECZH6

Investigate and implement IT security

Developed by	Skills for Justice
Version number	1
Date approved	February 2006
Indicative review date	February 2008
Validity	Current
Status	Imported
Originating organisation	Skills for Security
Original URN	SfJ ZH6
Relevant occupations	Public Services; Information and Communication Technology; ICT for practitioners; Financial Institution and Office Manager; Public Service Professionals; IT Service Delivery Occupations; Public Service and Other Associate Professionals
Suite	Countering E-Crime
Key words	investigate IT security, implement IT security, security recommendation