**Vendor:** EXIN

**Exam Code:** ISFS

**Exam Name:** Information Security Foundation based on ISO/IEC 27002

**Version:** DEMO

**QUESTION NO: 1**
You are the owner of the courier company SpeeDelivery. You employ a few people who, while waiting to make a delivery, can carry out other tasks. You notice, however, that they use this time to send and read their private mail and surf the Internet. In legal terms, in which way can the use of the Internet and e-mail facilities be best regulated?
A. Installing an application that makes certain websites no longer accessible and that filters attachments in e-mails
B. Drafting a code of conduct for the use of the Internet and e-mail in which the rights and obligations of both the employer and staff are set down
C. Implementing privacy regulations
D. Installing a virus scanner
**Answer: B**

**QUESTION NO: 2**
Why is air-conditioning placed in the server room?
A. In the server room the air has to be cooled and the heat produced by the equipment has to be extracted. The air in the room is also dehumidified and filtered.
B. When a company wishes to cool its offices, the server room is the best place. This way, no office space needs to be sacrificed for such a large piece of equipment.
C. It is not pleasant for the maintenance staff to have to work in a server room that is too warm.
D. Backup tapes are made from thin plastic which cannot withstand high temperatures. Therefore, if it gets too hot in a server room, they may get damaged.
**Answer: A**

**QUESTION NO: 3**
Who is authorized to change the classification of a document?
A. The author of the document
B. The administrator of the document
C. The owner of the document
D. The manager of the owner of the document
**Answer: C**

**QUESTION NO: 4**
The company Midwest Insurance has taken many measures to protect its information. It uses an Information Security Management System, the input and output of data in applications is validated, confidential documents are sent in encrypted form and staff use tokens to access information systems. Which of these is not a technical measure?
A. Information Security Management System
B. The use of tokens to gain access to information systems

C. Validation of input and output data in applications

D. Encryption of information

**Answer: A**

**QUESTION NO: 5**

What is an example of a physical security measure?

A. A code of conduct that requires staff to adhere to the clear desk policy, ensuring that confidential information is not left visibly on the desk at the end of the work day

B. An access control policy with passes that have to be worn visibly

C. The encryption of confidential information

D. Special fire extinguishers with inert gas, such as Argon

**Answer: D**

**QUESTION NO: 6**

What physical security measure is necessary to control access to company information?

A. Air-conditioning

B. Username and password

C. The use of break-resistant glass and doors with the right locks, frames and hinges

D. Prohibiting the use of USB sticks

**Answer: C**

**QUESTION NO: 7**

Why do organizations have an information security policy?

A. In order to demonstrate the operation of the Plan-Do-Check-Act cycle within an organization.

B. In order to ensure that staff do not break any laws.

C. In order to give direction to how information security is set up within an organization.

D. In order to ensure that everyone knows who is responsible for carrying out the backup procedures.

**Answer: C**

**QUESTION NO: 8**

You work in the IT department of a medium-sized company. Confidential information has got into the wrong hands several times. This has hurt the image of the company. You have been asked to propose organizational security measures for laptops at your company. What is the first step that you should take?

A. Formulate a policy regarding mobile media (PDAs, laptops, smartphones, USB sticks)

B. Appoint security personnel

C. Encrypt the hard drives of laptops and USB sticks

D. Set up an access control policy

**Answer: A**

**QUESTION NO: 9**

You work for a large organization. You notice that you have access to confidential information that you should not be able to access in your position. You report this security incident to the helpdesk.

The incident cycle isinitiated. What are the stages of the security incident cycle?

A. Threat, Damage, Incident, Recovery

B. Threat, Damage, Recovery, Incident

C. Threat, Incident, Damage, Recovery

D. Threat, Recovery, Incident, Damage

**Answer: C**

**QUESTION NO: 10**

Your organization has an office with space for 25 workstations. These workstations are all fully equipped and in use. Due to a reorganization 10 extra workstations are added, 5 of which are used for a call centre 24 hours per day. Five workstations must always be available. What physical security measures must be taken in order to ensure this?

A. Obtain an extra office and set up 10 workstations. You would therefore have spare equipment that can be used to replace any non-functioning equipment.

B. Obtain an extra office and set up 10 workstations. Ensure that there are security personnel both in the evenings and at night, so that staff can work there safely and securely.

C. Obtain an extra office and connect all 10 new workstations to an emergency power supply and UPS (Uninterruptible Power Supply). Adjust the access control system to the working hours of the new staff. Inform the building security personnel that work will also be carried out in the evenings and at night.

D. Obtain an extra office and provide a UPS (Uninterruptible Power Supply) for the five most important workstations.

**Answer: C**

**QUESTION NO: 11**

Which of the following measures is a preventive measure?

A. Installing a logging system that enables changes in a system to be recognized

B. Shutting down all internet traffic after a hacker has gained access to the company systems

C. Putting sensitive information in a safe

D. Classifying a risk as acceptable because the cost of addressing the threat is higher than the value of the information at risk

**Answer: C**

**QUESTION NO: 12**

What is a risk analysis used for?

A. A risk analysis is used to express the value of information for an organization in monetary terms.
B. A risk analysis is used to clarify to management their responsibilities.
C. A risk analysis is used in conjunction with security measures to reduce risks to an acceptable level.
D. A risk analysis is used to ensure that security measures are deployed in a cost-effective and timely fashion.
**Answer: D**

**QUESTION NO: 13**
A well executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives. What is not one of the four main objectives of a risk analysis?
A. Identifying assets and their value
B. Determining the costs of threats
C. Establishing a balance between the costs of an incident and the costs of a security measure
D. Determining relevant vulnerabilities and threats
**Answer: B**

**QUESTION NO: 14**
What is an example of a security incident?
A. The lighting in the department no longer works.
B. A member of staff loses a laptop.
C. You cannot set the correct fonts in your word processing software.
D. A file is saved under an incorrect name.
**Answer: B**

**QUESTION NO: 15**
Which of the following measures is a corrective measure?
A. Incorporating an Intrusion Detection System (IDS) in the design of a computer centre
B. Installing a virus scanner in an information system
C. Making a backup of the data that has been created or altered that day
D. Restoring a backup of the correct database after a corrupt copy of the database was written over the original
**Answer: D**