

SSCP^{Q&As}

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/sscp.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

- A. SSH (Secure Shell)
- B. S/MIME (Secure MIME)
- C. SET (Secure Electronic Transaction) D. SSL (Secure Sockets Layer)

Correct Answer: C

As protocol was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. It is comprised of three different pieces of software, running on the customer's PC (an electronic wallet), on the merchant's Web server and on the payment server of the merchant's bank. The credit card information is sent by the customer to the merchant's Web server, but it does not open it and instead digitally signs it and sends it to its bank's payment server for processing.

The following answers are incorrect because :

SSH (Secure Shell) is incorrect as it functions as a type of tunneling mechanism that provides terminal like access to remote computers.

S/MIME is incorrect as it is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.

SSL is incorrect as it uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication.

Reference : Shon Harris AIO v3 , Chapter-8: Cryptography , Page : 667-669

QUESTION 2

What is the main purpose of Corporate Security Policy?

- A. To transfer the responsibility for the information security to all users of the organization
- B. To communicate management's intentions in regards to information security
- C. To provide detailed steps for performing specific actions
- D. To provide a common framework for all development activities

Correct Answer: B

A Corporate Security Policy is a high level document that indicates what are management's intentions in regard to Information Security within the organization. It is high level in purpose, it does not give you details about specific products that would be use, specific steps, etc.. The organization's requirements for access control should be defined and documented in its security policies. Access rules and rights for each user or group of users should be clearly stated in an access policy statement. The access control policy should minimally consider:

Statements of general security principles and their applicability to the organization

Security requirements of individual enterprise applications, systems, and services

Consistency between the access control and information classification policies of different systems and networks

Contractual obligations or regulatory compliance regarding protection of assets

Standards defining user access profiles for organizational roles

Details regarding the management of the access control system

As a Certified Information System Security Professional (CISSP) you would be involved directly in the drafting and coordination of security policies, standards and supporting guidelines, procedures, and baselines.

Guidance provided by the CISSP for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed by the CISSP as well.

The following are incorrect answers:

To transfer the responsibility for the information security to all users of the organization is bogus. You CANNOT transfer responsibility, you can only transfer authority. Responsibility will also sit with upper management. The keywords ALL and USERS is also an indication that it is the wrong choice.

To provide detailed steps for performing specific actions is also a bogus detractor. A step by step document is referred to as a procedure. It details how to accomplish a specific task. To provide a common framework for all development activities is also an invalid choice. Security Policies are not restricted only to development activities.

Reference Used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1551-1565). Auerbach Publications. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 9109-9112). Auerbach Publications. Kindle Edition.

QUESTION 3

Preservation of confidentiality within information systems requires that the information is not disclosed to: A. Authorized person

B. Unauthorized persons or processes.

C. Unauthorized persons.

D. Authorized persons and processes

Correct Answer: B

Confidentiality assures that the information is not disclosed to unauthorized persons or processes.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 31.

QUESTION 4

A prolonged power supply that is below normal voltage is a:

- A. brownout
- B. blackout
- C. surge
- D. fault

Correct Answer: A

A prolonged power supply that is below normal voltage is a brownout.

From: HARRIS, Shon, All-In-One CISSP Certification uide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 5

What can best be defined as high-level statements, beliefs, goals and objectives?

- A. Standards
- B. Policies
- C. Guidelines
- D. Procedures

Correct Answer: B

Policies are high-level statements, beliefs, goals and objectives and the general means for their attainment for a specific subject area. Standards are mandatory activities, action, rules or regulations designed to provide policies with the support structure and specific direction they require to be effective. Guidelines are more general statements of how to achieve the policies objectives by providing a framework within which to implement procedures. Procedures spell out the specific steps of how the policy and supporting standards and how guidelines will be implemented.

Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

[Latest SSCP Dumps](#)

[SSCP Practice Test](#)

[SSCP Brindumps](#)