



Free Questions for ISSMP by certsdeals

Shared by Peters on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

Options:

A- No

B- Yes

Answer:

B

Explanation:

Sarah is guilty under copyright laws because pleading ignorance of copyright infringement is not an excuse.

What is copyright?

A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.

Question 2

Question Type: MultipleChoice

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

Options:

- A- Network security policy
- B- Backup policy
- C- Privacy policy
- D- User password policy

Answer:

C

Explanation:

Monitoring the computer hard disks or e-mails of employees pertains to the privacy policy of an organization.

Answer option B is incorrect. The backup policy of a company is related to the backup of its data.

Answer option A is incorrect. The network security policy is related to the security of a company's network.

Answer option D is incorrect. The user password policy is related to passwords that users provide to log on to the network.

Question 3

Question Type: MultipleChoice

Which of the following is a name, symbol, or slogan with which a product is identified?

Options:

A- Copyright

B- Trademark

C- Trade secret

D- Patent

Answer:

B

Explanation:

A trademark is a name, symbol, or slogan with which a product is identified. Its uniqueness makes the product noticeable among the same type of products. For example, Pentium and Athlon are brand names of the CPUs that are manufactured by Intel and AMD, respectively.

The trademark law protects a company's trademark by making it illegal for other companies to use it without taking prior permission of the trademark owner. A trademark is registered so that others cannot use identical or similar marks.

Answer option C is incorrect. A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information.

Answer option A is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.

Answer option D is incorrect. A patent is a set of exclusive rights granted to anyone who invents any new and useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

Question 4

Question Type: MultipleChoice

Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

Options:

- A- Packet filtering
- B- Tunneling
- C- Packet sniffing
- D- Spoofing

Answer:

B

Explanation:

Tunneling is a process used by remote users to make a secure connection to internal resources after establishing an Internet connection. The tunnel is created between the two ends by encapsulating the data in a mutually agreed-upon protocol for transmission.

Answer option A is incorrect. Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet.

Answer option C is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

Answer option D is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.

Question 5

Question Type: MultipleChoice

In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

Options:

A- Mobile Site

B- Cold Site

C- Warm Site

D- Hot Site

Answer:

D

Explanation:

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. It provides the backup facility, which is maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility.

A hot site is a backup site in case disaster has taken place in a data center. A hot site is located off site and provides the best protection. It is an exact replica of the current data center. In case a disaster struck to the data center, administrators just need to take the backup of

recent

data in hot site and the data center is back online in a very short time. It is very expensive to create and maintain the hot site. There are lots of third party companies that provide disaster recovery solutions by maintaining hot sites at their end.

Answer option B is incorrect. A cold site is a backup site in case disaster has taken place in a data center. This is the least expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It can be on site or off site.

Answer option A is incorrect. Mobile sites are self-reliant, portable shells custom-fitted with definite telecommunications and IT equipment essential to meet system requirements. These are presented for lease through commercial vendors.

Answer option C is incorrect. A warm site is, quite logically, a compromise between hot and cold sites. Warm sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. These sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

Question 6

Question Type: MultipleChoice

Which of the following are known as the three laws of OPSEC?

Each correct answer represents a part of the solution. Choose three.

Options:

- A- If you don't know the threat, how do you know what to protect?
- B- If you don't know what to protect, how do you know you are protecting it?
- C- If you are not protecting it (the critical and sensitive information), the adversary wins!
- D- If you don't know about your security resources you cannot protect your network.

Answer:

A, B, C

Explanation:

OPSEC is also known as operations security. It has three laws.

The First Law of OPSEC. If you don't know the threat, how do you know what to protect? Although specific threats may vary from site to site or program to program. Employees must be aware of the actual and postulated threats. In any given situation, there is likely to be more than one adversary, although each may be interested in different information.

The Second Law of OPSEC. If you don't know what to protect, how do you know you are protecting it? The 'what' is the critical and sensitive, or target, information that adversaries require to meet their objectives.

The Third Law of OPSEC. If you are not protecting it (the critical and sensitive information), the adversary wins! OPSEC vulnerability assessments, (referred to as 'OPSEC assessments' - OA's - or sometimes as Surveys') are conducted to determine whether or not critical information is vulnerable to exploitation. An OA is a critical analysis of 'what we do' and 'how we do it' from the perspective of an adversary. Internal procedures and information sources are also reviewed to determine whether there is an inadvertent release of sensitive information.

Answer option D is incorrect. The statement given in the option is not a valid law of OPSEC.

Question 7

Question Type: FillInTheBlank

Fill in the blank with an appropriate word. _____ are used in information security to formalize security policies.

Answer:

Question 8

Question Type: MultipleChoice

You work as the project manager for Bluewell Inc. You are working on NGQQ Project for your company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

Options:

- A- Risk mitigation
- B- Risk acceptance
- C- Risk avoidance
- D- Risk transference

Answer:

D

Explanation:

Risk transference is a risk response planning technique that is used to shift the impact of a threat to a third party, together with the ownership of the response.

Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost-effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows.

Risk acceptance. It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy.

Risk avoidance. It is a technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact.

Risk mitigation. It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an acceptable threshold.

Risk transference. It is used to shift the impact of a threat to a third party, together with the ownership of the response.

Question 9

Question Type: MultipleChoice

Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?

Options:

- A- Internet Crimes Against Children (ICAC)
- B- Project Safe Childhood (PSC)
- C- Anti-Child Porn.org
- D- Innocent Images National Initiative (IINI)

Answer:

B

Explanation:

Project Safe Childhood (PSC) is a Department of Justice initiative launched in 2006 that aims to combat the proliferation of technology-facilitated sexual exploitation crimes against children. PSC coordinates efforts by various federal, state and local agencies and organizations to protect children by investigating and prosecuting online sexual predators. PSC partners include Internet Crimes Against Children (ICAC) task forces, the FBI, U.S. Postal Inspection Service, Immigration and Customs Enforcement, the U.S. Marshals Service, the National Center for Missing & Exploited Children, and state and local law enforcement officials in each U.S. Attorney's district. PSC also helps local communities to create programs and develop strategies to investigate child exploitation.

Answer option A is incorrect. Internet Crimes Against Children (ICAC) is a task-force started by the United States Department of Justice's Office of Juvenile Justice and Delinquency Prevention (OJJDP) in 1998. Its primary goals are to provide state and local law enforcement agencies the tools to prevent Internet crimes against children by encouraging multi-jurisdictional cooperation as well as educating both law enforcement agents and parents and teachers. The aims of ICAC task forces are to catch distributors of child

pornography on the Internet, whether delivered on-line or solicited on-line and distributed through other channels and to catch sexual predators who solicit victims on the

Internet through chat rooms, forums and other methods. Currently all fifty states participate in ICAC.

Answer option C is incorrect. Anti-Child Porn.org (ACPO) is an organization, which has members all over the world, focusing on the topics related to child exploitation, online predators, and child pornography. Its Web site provides necessary information for law enforcement to

parents, and other interested organizations. It also provides software such as Reveal, which can be used to evaluate and check files on a computer for explicit or illegal contents.

Answer option D is incorrect. Innocent Images National Initiative (IINI) is an organization, which is developed by the FBI as part of its Cyber Crimes program. This organization is established for the purpose of identifying, investigating, and prosecuting people who use computers for sexual exploitation of children and child pornography. While performing these tasks, IINI also try to identify and release children being exploited.

Question 10

Question Type: MultipleChoice

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

Options:

A- Availability

B- Non-repudiation

C- Integrity

D- Confidentiality

Answer:

C

Explanation:

Integrity refers to the ability to ensure that the data is not modified or tampered with.

Integrity means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a Web site, when someone is able to cast a very large number of votes in an online poll, and so on.

Answer option D is incorrect. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a

company's employees is stolen or sold, it could result in a breach of confidentiality.

Answer option A is incorrect. Availability means that data must be available whenever it is needed.

Answer option B is incorrect. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to

any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

To Get Premium Files for ISSMP Visit

<https://www.p2pexams.com/products/issmp>

For More Free Questions Visit

<https://www.p2pexams.com/isc2/pdf/issmp>

