

Exam Report: 3.1.8 Practice Questions

Date: 1/14/2020 11:58:58 am
Time Spent: 4:43

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 87%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following is defined as a contract that prescribes the technical support or business parameters a provider will bestow to its client?

- ☐ Final audit report
- ➡ ☒ Service level agreement
- ☐ Certificate practice statement
- ☐ Mutual aid agreement

Explanation

A service level agreement is defined as a contract that prescribes the technical support or business parameters a provider will bestow to its client.

A mutual aid agreement is an agreement between two organizations to support each other in the event of a disaster. A final audit report is the result of an external auditor's inspection and analysis of an organization's security status. A certificate practice statement defines the actions and promises of a certificate service authority.

References

LabSim for Security Pro, Section 3.1.
[All Questions SecPro2017_v6.exm SECURE_POL_01]

▼ Question 2: Correct

HIPAA is a set of federal regulations that define security guidelines. What do HIPAA guidelines protect?

- ☐ Non-repudiation
- ☐ Integrity
- ☐ Availability
- ➡ ☒ Privacy

Explanation

HIPAA is a set of federal regulations that enforce the protection of privacy. Specifically, HIPAA protects the privacy of medical records.

References

LabSim for Security Pro, Section 3.1.
[All Questions SecPro2017_v6.exm SECURE_POL_02]

▼ Question 3: Correct

What is a service level agreement (SLA)?

- ☐ A contract with a legal entity to limit your asset loss liability
- ☐ A contract with an ISP for a specific level of bandwidth
- ➔ ☒ A guarantee of a specific level of service
- ☐ An agreement to support another company in the event of a disaster

Explanation

An SLA is a guarantee of a specific level of service from a vendor. That service may be communication links, hardware, or operational services. An SLA is a form of insurance against disasters or security intrusions that may affect your organization's mission-critical business functions.

An agreement to support another company in the event of a disaster is known as a mutual aid agreement. A contract with a legal entity to limit your asset loss liability is an insurance policy. A contract with an ISP for a specific level of bandwidth is a service contract.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_03]

▼ Question 4: Incorrect

A Service Level Agreement (SLA) defines the relationship and contractual responsibilities of providers and service recipients. Which of the following characteristics are most important when designing an SLA? (Select two.)

- ☐ Employee vetting procedures that don't apply to contract labor.
- ☒ ~~Industry standard templates for all SLAs to ensure corporate compliance.~~
- ➔ ☐ Detailed provider responsibilities for all continuity and disaster recovery mechanisms.
- ➔ ☒ Clear and detailed descriptions of penalties if the level of service is not provided.

Explanation

A Service Level Agreement (SLA) should define, with sufficient detail, any penalties incurred if the level of service is not maintained. In the information security realm, it is also vital that the provider's role in disaster recovery operations and continuity planning is clearly defined. Industry standard templates are frequently used as a starting point for SLA design, but must be tailored to the specific project or relationship to be effective.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_04]

▼ Question 5: Incorrect

You plan to implement a new security device on your network. Which of the following policies outlines the process you should follow before implementing that device?

- ☒ ~~Acceptable use~~
- ☐ Resource allocation
- ☐ SLA
- ➔ ☐ Change management

Explanation

A *change and configuration management policy* provides a structured approach to securing company assets and making changes. Change management:

- Establishes hardware, software, and infrastructure configurations that are universally deployed

throughout the corporation.

- Tracks and documents significant changes to the infrastructure.
- Assesses the risk of implementing new processes, hardware, or software.
- Ensures that proper testing and approval processes are followed before changes are allowed.

An *Acceptable Use Policy* (AUP) identifies employees rights to use company property, such as internet access and computer equipment, for personal use. A *resource allocation policy* outlines how resources are allocated. Resources could include staffing, technology, or budgets. Service Level Agreements (SLAs), sometimes called maintenance contracts, guarantee the quality of a service to a subscriber by a network service provider.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_08]

▼ Question 6: Correct

When you inform an employee that they are being terminated, what is the most important activity?

- ☐ Allowing them to collect their personal items
- ➡ ☒ Disabling their network access
- ☐ Allowing them to complete their current work projects
- ☐ Giving them two weeks' notice

Explanation

When an employee is terminated, you should disable their network access immediately. Often, an employee is taken into an exit interview where they are informed of the termination and asked to review their NDA and other security agreements. While the exit interview is occurring, the system administrator disables the user's network access and security codes.

Returning personal items is the least important task when removing an employee. Terminated employees should not be allowed to complete work projects, nor should they be given two week's notice. Both of these activities grant the ex-employee the ability to cause damage to your secure environment as a form of retaliation.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_10]

▼ Question 7: Correct

What is the most effective way to improve or enforce security in any environment?

- ☐ Enforcing account lockout
- ➡ ☒ Providing user-awareness training
- ☐ Requiring two-factor authentication
- ☐ Disabling Internet access

Explanation

The most effective way to improve and enforce security in any environment is user awareness training. If users are educated about security and how to perform their work tasks securely, the overall security of the environment improves.

Enforcing account lockout, two-factor authentication, and disabling Internet access are all valid security countermeasures or improvements. However, they do not have as large a positive impact on overall security as user awareness training.

References


LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_12]

▼ Question 8: Correct

You have a set of DVD-RW discs that have been used to archive files for your latest development project. You need to dispose of the discs.

Which of the following methods should you use to best prevent data extraction from the discs?

- ☐ Degauss the disks
-  ☒ Shred the disks
- ☐ Delete the data on the discs
- ☐ Write junk data over the discs seven times

Explanation

To completely prevent reading data from discs, destroy them using a DVD shredder or crusher.

Degaussing works for magnetic media such as floppy and hard disk drives. Simply deleting data offers little protection. Writing junk data over the media sanitizes the discs by removing data remanence.


References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_14]

▼ Question 9: Correct

Which of the following best describes the concept of *due care* or *due diligence*?

-  ☒ Reasonable precautions based on industry best practices are utilized and documented.
- ☐ Legal disclaimers are consistently and conspicuously displayed on all systems.
- ☐ Security through obscurity is best accomplished by port stealthing.
- ☐ Availability supersedes security unless physical harm is likely.

Explanation

Due care or *due diligence* are legal terms that describe the responsibility of one party to act reasonably in relation to the rights of another. In this example, due care is best described as the utilization and documentation of reasonable precautions based on industry best practices. The subjective nature of the term 'reasonable' is frequently determined by courts. Any deviation from accepted industry best practices may subject an organization or individual to legal action based on these grounds.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_15]

▼ Question 10: Correct

Which of the following is an example of a strong password?

- ☐ desktop#7
- ☐ Robert694
-  ☒ a8bT11\$yi
- ☐ at9iov45a

Explanation

A strong password should not contain dictionary words or any part of the login name. They should include upper and lower-case letters, numbers, and symbols. In addition, longer passwords are stronger than shorter passwords.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_16]

▼ Question 11: Correct

Which of the following is a recommendation to use when a specific standard or procedure does not exist?

- ☐ Standard
- ☐ Procedure
- ☐ Baseline

➡ ☒ Guideline

Explanation

A *guideline* is a recommendation to use when a specific standard or procedure does not exist.

A *standard* is a legal, industry, or best business practice that a company implements, such as building codes. A *baseline* dictates the settings and security mechanisms that must be imposed on a system in order to comply with required security standards. A *procedure* is a detailed, specific step-by-step instruction for a process.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_21]

▼ Question 12: Correct

Which of the following is the best protection against security violations?

- ☐ Fortress mentality
- ☐ Bottom-up decision-making
- ➡ ☒ Defense in-depth
- ☐ Monolithic security

Explanation

Defense in-depth is the best protection against security violations.

Monolithic security and fortress mentality are both poor security perspectives, as they rely upon a single protection mechanism. Bottom-up decision-making is a poor security process, as it does not firmly establish responsibility, management control, or standards enforcement. Ultimately, such a process will lead to chaos rather than security.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_22]

▼ Question 13: Correct

What is the primary purpose of source code escrow?

- ☐ To provide a backup copy of software to use for recovery in the event of a disaster
- ➡ ☒ To obtain change rights over software after the vendor goes out of business
- ☐ To hold funds in reserve for unpredicted costs before paying the fees of the programmer
- ☐ To obtain resale rights over software after the vendor goes out of business

Explanation

Source code escrow is used to obtain change rights over software after the vendor goes out of business.

Source code escrow is not used to obtain resale rights, backup software, or withhold funds from programmers.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_25]

▼ Question 14: Correct

Change control should be used to oversee and manage changes over what aspect of an organization?

- ➡ ☒ Every aspect
- ☐ Physical environment
- ☐ IT hardware and software
- ☐ Personnel and policies

Explanation

Every aspect of an organization should be monitored and managed by change control.

Focusing only on hardware and software, personnel and policies, or the physical environment will limit the effectiveness of change control. Change control should cover the entire organization.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_27]

▼ Question 15: Correct

You have recently discovered that a network attack has compromised your database server. The attacker may have stolen customer credit card numbers.

You have stopped the attack and implemented security measures to prevent the same incident from occurring in the future. What else might you be legally required to do?

- ☐ Implement training for employees who handle personal information
- ☐ Perform additional investigations to identify the attacker
- ☐ Delete personally identifiable information from your computers
- ➡ ☒ Contact your customers to let them know about the security breach

Explanation

After you have analyzed the attack and gathered evidence, be aware that, in some states, you are required to notify individuals if their personal information might have been compromised. For example, if an incident involves the exposure of credit card numbers, identifying information (such as Social Security numbers), or medical information, you might be legally obligated to notify potential victims and take measures to help protect their information from further attack.

References

LabSim for Security Pro, Section 3.1.

[All Questions SecPro2017_v6.exm SECURE_POL_09]