OutSystems
Security-Specialist
Security Specialist (OutSystems 11)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

How does OutSystems address the requirement of audit controls under HIPAA Technical safeguards to track and monitor access to EPHI?

A. OutSystems only logs successful access attempts, neglecting failed attempts.
B. Audit controls are not a concern for OutSystems, as it focuses solely on application development.
C. OutSystems includes a robust audit trail feature, capturing and logging all activities related to ePHI access.
D. OutSystems relies on external audit tools, and it does not have built-in audit controls.

Answer: C

Question: 2

When configuring security contacts in the OutSystems support portal, what is a critical consideration to prevent unauthorized access?

A. Security contacts do not impact portal access.
B. Share login credentials with team members for efficient collaboration.
C. Ensure that user roles and permissions are synchronized with the external provider.
D. Implement two-factor authentication for enhanced security.
E. Disable multi-factor authentication for a smoother user experience.
F. Assign the "Administrator" role to all support portal users.

Answer: D

Question: 3

OutSystems by default gives the built-in logic for end-user authentication and respective configuration. Other than the built-in logic, what are the other mechanisms?

A. LDAP
B. All of the above
C. SAML 2.0 and AZURE AD
D. Active Directory

Answer: B

Question: 4

In the context of hardening the OutSystems Platform Server, what is a best practice for securing access to the Service Center?

A. Restrict access to the Service Center to specific IP addresses.
B. Disable Service Center access for enhanced security.
C. Use default Service Center credentials for convenience.
D. Allow anonymous access to simplify user management.

Answer: A

Question: 5

When developing healthcare applications in OutSystems, what is a critical consideration for ensuring HIPAA compliance in terms of data storage?

A. Store all patient data in plain text for easy retrieval.
B. Implement encryption for data at rest and in transit.
C. Rely on the default security features of the OutSystems platform.
D. Avoid data encryption to improve application performance.

Answer: B

Question: 6

When configuring an External Authentication Provider in OutSystems, what is a potential security risk that should be mitigated to prevent unauthorized access?

A. Share external provider credentials with end-users for troubleshooting purposes
B. Disable multi-factor authentication for a smoother user experience
C. Ensure that user roles and permissions are synchronized with the external provider
D. Allow any user from the external provider to access the OutSystems application

Answer: D

Question: 7

When configuring OutSystems Platform Server backups for disaster recovery, what should be avoided to prevent potential security risks?

A. Disable backup procedures to reduce resource usage.
B. Rely on default backup settings for simplicity.
C. Implement regular backups for data redundancy.
D. Store backups in an unsecured location.

Answer: D

Question: 8

In a scenario where an application experiences frequent brute force attacks, what is a potential pitfall when relying solely on CAPTCHA for protection?

A. CAPTCHA is only effective against manual brute force attacks.
B. CAPTCHA introduces significant user friction.
C. CAPTCHA can be easily bypassed by automated tools.
D. CAPTCHA is a foolproof solution with no associated pitfalls.

Answer: C

Question: 9

In a multi-server deployment of an OutSystems application, what consideration should be taken into account when configuring secure session cookies?

A. Use a shared session cookie across all servers for consistency.
B. Each server manages its own session cookies independently.
C. Disable secure session cookies for better load balancing.
D. The platform automatically handles session cookies in multi-server environments.

Answer: D

Question: 10

In the context of Brute Force Protection for IT Users, what is a potential pitfall when configuring IP-based blocking?

A. Implement whitelisting for all known IP addresses.
B. Avoid dynamic IP blocking to prevent false positives.
C. Block all IP addresses to ensure maximum security.
D. Use a fixed IP blocking duration for all blocked addresses.

Answer: B

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/