Exam4Future

Salesforce Security & Privacy Accredited Professional Exam

Salesforce Security-and-Privacy-Accredited-Professional

Version Demo

Total Demo Questions: 13

Total Premium Questions: 135

Buy Premium PDF

https://exam4future.com

support@exam4future.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security and Privacy Fundamentals	1
Topic 2, Data Governance	10
Topic 3, Data Privacy	28
Topic 4, Security	95
Topic 5, Mix Questions	1
Total	135

QUESTION NO: 1

How much Heroku data storage is included with Privacy Center?

A. 1.5 TB

B. 5TB

C. 1TB

D. 3TB

ANSWER: A

Explanation:

Privacy Center includes **1.5 TB** of Heroku data storage. This storage supports the Privacy Center application's processing and management of privacy-related work, such as receiving and orchestrating data-subject requests, locating relevant personal data, and retaining the operational information needed to complete those requests. The entitlement is specifically associated with the Heroku-based services that underpin Privacy Center, rather than being ordinary Salesforce org data storage or a separately purchased general-purpose Heroku allocation.

When planning a Privacy Center implementation, teams should account for this included capacity in relation to the expected request volume, the number of connected systems, retention requirements, and the amount of request-related data maintained by the solution. Salesforce's Privacy Center product information describes the service's role in helping organizations operationalize privacy-request management and automate privacy processes. See the Salesforce Privacy Center overview and Salesforce's Privacy Center documentation for product and implementation guidance.

QUESTION NO: 2

10. Can a customer run a penetration test against Salesforce?

A. Some types of penetration testing are permitted, but not in production

B. No, this is not permitted under any circumstances

C. Penetration testing is allowed, but the Salesforce Agreement needs to be signed before testing can commence

D. Penetration testing can be carried out at anytime by anyone

ANSWER: C

Explanation:

Penetration testing is allowed, but the Salesforce Agreement needs to be signed before testing can commence. Salesforce permits customers to assess the security of their own Salesforce environments when the activity is performed within the contractual and policy framework that governs use of the service. A signed Salesforce Agreement establishes the customer's authorized use of the platform and the applicable obligations for both parties before security testing begins. This is important because penetration testing can involve high-volume requests, scanning, or attempts to identify vulnerabilities; those activities must be controlled so they do not affect other tenants, shared infrastructure, service availability, or Salesforce personnel and systems outside the customer's authorized scope.

Customers and their authorized third-party testers should also follow Salesforce's Security Assessment Policy, including its scope, testing restrictions, and reporting requirements. Testing should be limited to the customer's own organization and authorized assets, conducted with appropriate safeguards, and handled in accordance with the policy's vulnerability-disclosure process. The governing agreement and the Security Assessment Policy together provide the authorization and operational boundaries needed to conduct an assessment responsibly. See Salesforce's Security Assessment Policy and its customer agreements.

QUESTION NO: 3

Within Data Mask a user wants to stop a configuration that is currently running. What dropdown option needs to be selected to terminate the execution

A. END

B. STOP

C. CANcEL

D. ABORT

ANSWER: D

Explanation:

ABORT is the dropdown action used to terminate a Data Mask configuration that is currently executing. Data Mask configurations can run asynchronously because they may process substantial volumes of records and apply masking rules across multiple objects. While a run is in progress, the configuration's actions menu provides the abort action so an authorized user can halt that active execution rather than wait for the job to complete. This is useful when a configuration was started unintentionally, a masking rule requires correction, or operational circumstances require the sandbox-refresh preparation process to stop. After aborting a run, administrators should review the configuration and job status before making changes or starting another execution, since records processed before the termination can already have been masked. Salesforce's security guidance emphasizes protecting nonproduction data through appropriate masking controls, and Data Mask is designed to provide those controls in sandbox environments. See Salesforce's Data Mask documentation and the Salesforce security implementation guidance for data masking.

QUESTION NO: 4

What is the primary difference between Data Mask and Data Encryption?

A. Data encryption is used for masking data in a production environment

B. Data encryption is an add on feature to the Data Mask product

C. Data encryption prevents malicious attackers from accessing or interacting with sensitive data at rest in the data center.

D. Data masking prevents developers or other users from viewing sensitive data in the user interface or exporting it as plain text

ANSWER: C

Explanation:

Data encryption prevents unauthorized parties from reading sensitive information if they obtain access to stored Salesforce data, whereas Salesforce Data Mask replaces sensitive values with realistic but non-sensitive values in sandbox copies. Salesforce Shield Platform Encryption protects data at rest by encrypting supported standard and custom fields, files, and other supported data using strong encryption. Authorized users can continue to work with decrypted values according to their permissions and the organization's encryption configuration, while the encrypted representation protects the stored data from unauthorized access at the infrastructure layer.

This distinction is important when an organization needs to safeguard production data in the event of an infrastructure compromise or unauthorized physical access to underlying storage. Encryption addresses that at-rest protection requirement. Salesforce documents that Platform Encryption encrypts sensitive data while preserving key platform functionality, and it is part of Salesforce Shield. More details are available in the Salesforce Platform Encryption overview and the Salesforce Data Mask documentation.

QUESTION NO: 5

You need to limit when and where from users can access Salesforce- to help reduce the risks of unauthorized access. How should you go about this.

A. Restrict Access based on Login IP Addresses but login hairs can't be set up in conjunction with this feature

B. Use MFA to help ensure users are using a more secure login process

C. Restrict access based on Login IP Addresses and use the Login Hours feature together

D. Do not allow users to access Salesforce from outside the office.

ANSWER: C

Explanation:

Restrict access based on Login IP Addresses and use the Login Hours feature together directly addresses both dimensions in the requirement: where users can sign in from and when they can sign in. Salesforce administrators can configure login IP ranges on profiles to define the network addresses from which assigned users are permitted to access Salesforce. This creates an enforceable location-based access boundary for the relevant user population. Administrators can also configure profile login hours, which define the days and times during which those users may log in. Outside the permitted schedule, Salesforce prevents login, reducing the opportunity for unauthorized access during periods when access is not expected or operationally necessary.

Applying both controls together follows a defense-in-depth approach. A successful login must occur from an approved network location and within an approved time window, helping organizations align Salesforce access with workplace, operational, or risk-management policies. These settings are managed at the profile level, so administrators can tailor the permitted IP ranges and schedules to the access needs of different groups of users. Salesforce documents these controls in its guidance for restricting login IP ranges and setting login hours.

QUESTION NO: 6

Which feature lets an administrator compare an org's security settings against a Salesforce standard or a custom baseline?

A. Health Check

B. Transaction Security

C. Data Mask

D. Login History

ANSWER: A

Explanation:

Health Check is correct. Health Check compares selected Salesforce security settings with a standard baseline or an organization-defined custom baseline and provides a score that indicates how closely the org aligns with that baseline. The results identify settings that differ from the target so administrators can prioritize remediation.

Health Check is designed for security-configuration assessment. It does not provide real-time user activity monitoring or replace the need to review permissions, sharing settings, and operational controls. See Salesforce's Health Check documentation.

QUESTION NO: 7

Which three capabilities are part of the Health Check tool?

A. Align your org's security setting with Salesforce-recommended security standards

B. Organize user access logs

C. Access event log files to track user activity and feature adoption and troubleshoot issues

D. Verify that multiple Salesforce applications have the same level of security

E. Compare your org's security settings against a custom security baseline.

F. Review a Health Check score and the settings that contribute to it.

ANSWER: A E F

Explanation:

Health Check helps administrators assess an individual Salesforce org's security configuration against a defined baseline. "Align your org's security setting with Salesforce-recommended security standards" is a core use case because Health Check compares configurable security settings with Salesforce's standard baseline, helping teams identify settings that need attention. Administrators can also "Compare your org's security settings against a custom security baseline." A custom baseline allows an organization to tailor the comparison to its own security requirements rather than relying solely on the Salesforce-recommended baseline. Finally, Health Check can "Review a Health Check score and the settings that contribute to it." The resulting score and detailed report provide a practical way to prioritize security configuration work and understand the current alignment with the selected baseline. These capabilities concern configuration assessment and remediation planning for the org. Salesforce documents that Health Check is available from Setup and supports standard or custom baselines for evaluating security settings. See Salesforce Health Check documentation and the Trailhead Health Check module.

QUESTION NO: 8

Which two date types are available when filtering on a condition that has the DATETIME object field?

A. Relative

B. Absolute

C. Within

D. Outside

ANSWER: A B

Explanation:

The available date types for a condition based on a DATETIME field are **Relative** and **Absolute**. Relative dates express a time period in relation to the current date and time, such as a rolling range based on the current day, week, month, or a specified number of prior days. This makes the condition dynamic: its effective time window updates automatically as time passes, which is useful for policies or filters intended to continuously evaluate recent activity.

Absolute dates identify a fixed, explicit date or date-time boundary. They are appropriate when the filter must apply to a specific historical or scheduled interval and must not shift over time. Salesforce supports date and date-time filtering semantics that distinguish fixed date values from relative date expressions; relative date literals are evaluated in relation to the current date, while explicit values provide fixed boundaries. This distinction allows administrators to configure conditions that either remain anchored to known timestamps or continue operating over a moving time period. See Salesforce's Date Formats and Date Literals documentation and the Salesforce report filtering guidance.

QUESTION NO: 9

Which three standard authentication protocols does Salesforce support to integrate external applications using APIs?

A. OpenID Connect

B. Single Sign On (SSO)

C. OMFA

D. Security Assertion Markup Language (SAML)

E. OAuth

ANSWER: A D E

Explanation:

Salesforce supports **OAuth**, **OpenID Connect**, and **Security Assertion Markup Language (SAML)** as industry-standard protocols for identity and access integration. OAuth is the core authorization framework used by external applications to obtain access tokens and call Salesforce APIs without handling a user's Salesforce password directly. Salesforce implements OAuth through connected apps and supported authorization flows, allowing an integration to request appropriately scoped access.

OpenID Connect builds on OAuth and provides a standard identity layer. It enables a relying application to authenticate a user and receive identity information in a signed ID token, which is useful when an integration needs both API authorization and verified user identity. Security Assertion Markup Language (SAML) uses signed assertions exchanged between an identity provider and Salesforce to establish trusted authentication, commonly in enterprise federation and single-sign-on architectures. Together, these protocols provide recognized, interoperable approaches for delegated API access, identity verification, and federated authentication. Salesforce's OAuth guidance is available in the OAuth overview, and its federation documentation describes SAML single sign-on.

QUESTION NO: 10

How do customers access Field Audit Trail data?

A. Event Log Files

B. Set-up Audit Trail

C. Salesforce API

D. Pre-built Tableau CRM app

ANSWER: C

Explanation:

Salesforce API is correct because Field Audit Trail stores older, archived field-history records in the `FieldHistoryArchive` object. Customers retrieve this archived audit data programmatically through Salesforce APIs, such as by querying the object with SOQL through the REST or SOAP API. This API-based access is particularly important when organizations need to retain field-history information beyond the standard field-history retention period for regulatory, legal, or internal audit purposes. Field Audit Trail is part of Salesforce Shield and lets an organization define a history-retention policy for tracked fields, retaining the resulting archived history for up to ten years. The archive is designed for retrieval and reporting processes that can query the historical records and use them in external compliance, investigation, or data-analysis workflows. Access to the data remains subject to the user's Salesforce permissions and the organization's sharing and security model, so API integrations should use appropriately authorized identities and follow least-privilege practices. Salesforce documents the archived history object and its API-query use in its Field Audit Trail guidance: Field Audit Trail and FieldHistoryArchive Object Reference.

QUESTION NO: 11

What are three implementation activities that should happen prior to enabling MFA for users?

A. Document processes and troubleshooting information

B. Enable the Salesforce Authenticator app for the org/tenant

C. Test registration and login flows for each supported verification method

D. Distribute verification methods and registration instructions to users

ANSWER: A C D

Explanation:

A successful MFA rollout requires operational preparation, validation, and user readiness before enforcement begins. Documenting processes and troubleshooting information establishes clear support procedures for common situations, such as a user obtaining a new phone, losing an authenticator device, or needing help completing registration. This preparation helps administrators and help-desk teams resolve access issues consistently while maintaining appropriate identity-verification controls.

Testing registration and login flows for every supported verification method verifies that the selected methods work as intended for the organization's users, devices, network conditions, and connected login scenarios. Testing should include the complete user experience, from enrollment through a successful MFA challenge, so implementation issues are found before MFA affects production access.

Distributing verification methods and registration instructions gives users adequate notice and practical guidance to enroll before the requirement takes effect. Clear communications should state the rollout timeline, approved verification methods, enrollment steps, and support contact path. Salesforce's MFA guidance emphasizes planning, testing, user communication, and support readiness as core rollout activities. See Salesforce Help: Multi-Factor Authentication and Trailhead: Multi-Factor Authentication.

QUESTION NO: 12

Which three controls help reduce the risk of unauthorized access from an active Salesforce session?

A. Session timeout

B. Lock sessions to the IP address from which they originated

C. Require HTTPOnly cookies

D. Password expiration

E. Password history

ANSWER: A B C

Explanation:

Session timeout, **Lock sessions to the IP address from which they originated**, and **Require HTTPOnly cookies** are session-security controls that help reduce misuse of an authenticated session. A session timeout limits the period in which an inactive session remains valid. Locking sessions to the originating IP address helps prevent reuse from a different network address. HTTPOnly cookies help prevent client-side scripts from accessing session cookies.

Password expiration and password history are credential-policy controls, not controls over an already established session. Salesforce documents these options in Session Security Settings.

QUESTION NO: 13

What are the two typical human emotions/reactions cyber criminals exploit to steal credentials and infiltrate your network?

A. Curiosity

B. Surprise

C. Fear

D. Rewards

ANSWER: A C

Explanation:

Curiosity and fear are common social-engineering triggers used in credential-theft campaigns. A message designed to provoke curiosity may promise access to unexpected information, such as a shared document, an invoice, a confidential file, or an account-related item. The recipient may click a link or open an attachment to satisfy that curiosity before verifying the sender or destination. Fear-based messages create pressure by warning that an account is locked, suspicious activity has occurred, a payment is overdue, or immediate action is needed. This urgency can cause people to bypass normal caution and enter credentials into a fraudulent sign-in page.

These tactics are effective because attackers are targeting human decision-making rather than attempting to defeat technical controls directly. Security awareness should reinforce pausing before acting, independently navigating to a known service instead of using an unsolicited link, and reporting suspicious messages. Salesforce's guidance emphasizes that phishing commonly uses urgency and convincing impersonation to obtain sensitive information, while its security resources describe social engineering as manipulation that exploits human behavior. See Salesforce phishing awareness guidance and Salesforce Security.