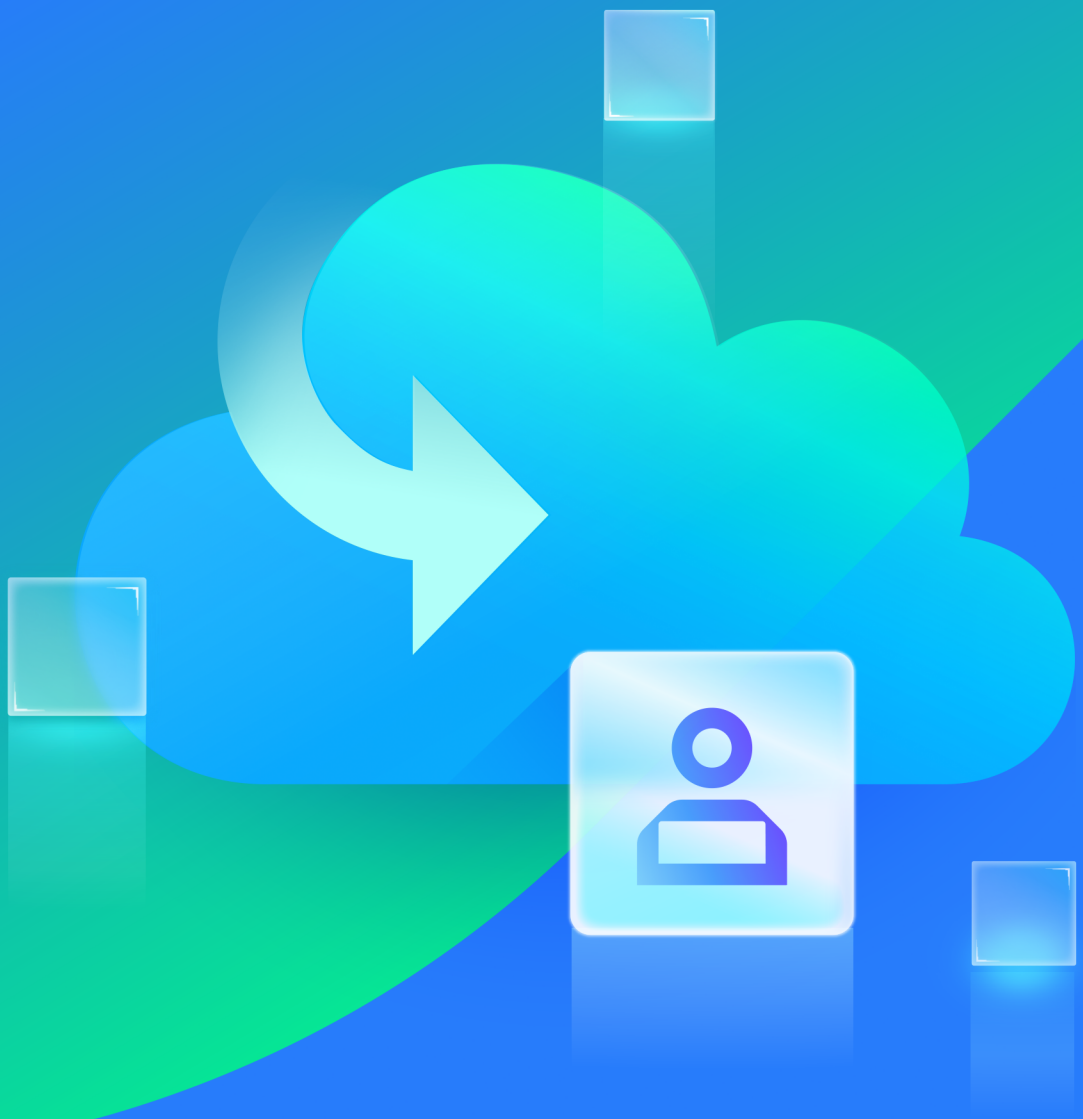
Salesforce Resilience Best Practices Guide



Introduction

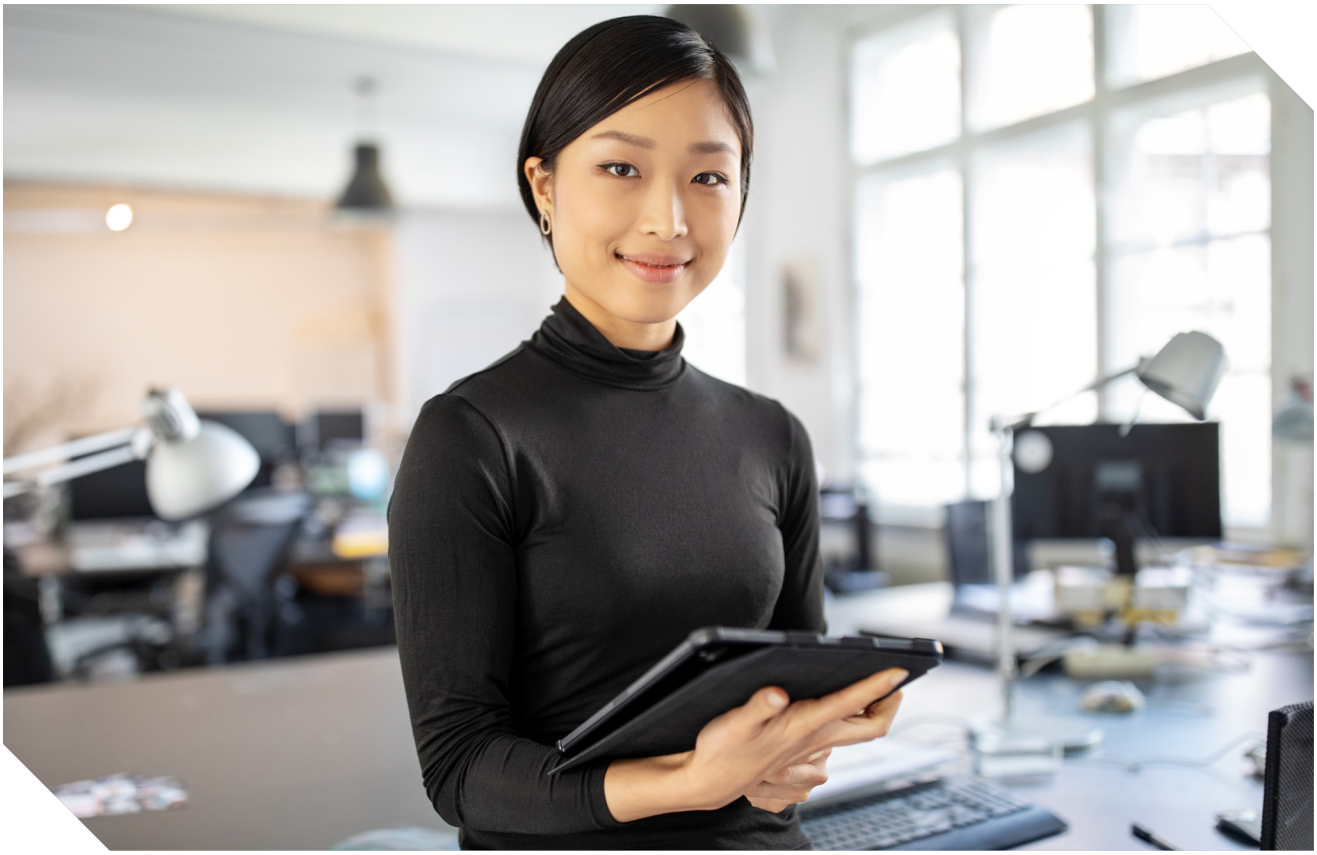
Data is key to any business today — it fuels decision-making, strengthens customer relationships, and empowers overall operations. As a leading customer relationship management (CRM) platform, businesses increasingly rely on Salesforce to drive growth and productivity. Salesforce has thus become a central hub for managing a company's invaluable data.

It is important to note that Salesforce uses a shared responsibility model. This model clearly defines the assumption of responsibility by Salesforce when you utilize their platform, and where you retain responsibility, namely, over your data. At a high level, Salesforce is in charge of the infrastructure, platform, and software, however the data and metadata is still your responsibility, including its protection and security.

This guide explores Salesforce backup and recovery best practices that organizations should follow to make sure their critical data is secure and accessible. We'll dive deep into the ins and outs of Salesforce backup, emphasizing your pivotal role in data loss prevention, security, and compliance.

Shared Responsibility Model

	Salesforce's responsibility	YOUR responsibility
Primary responsibility	**Cloud Service** Uptime and availability of the CRM application for all users	**YOUR Salesforce data and metadata** Control over your data residing in Salesforce
Supporting technology	**Data Replication** DC to DC geo-redundancy	**Salesforce backup** Copy of your data, stored in a different location, separated from the source
	Ecosystem tools Recycle bin and weekly export Data loader, sandboxes and Force.com migration tool	**Quick data loss recovery** Restore Salesforce records, hierarchies, fields, files and metadata
Protection	**Infrastructure-level** • Physical security • Logical security • App-level security • User/Admin controls	**Data-level** • Accidental deletion: Admin, developer, user or the over-privileged • Integration errors • Malicious or accidental data corruption
Compliance	**Role as data processor** • Data privacy • Regulatory controls • Industry certifications	**Role as data owner** • Answer to corporate and industry regulations • Payment details, confidential information (e.g., SSNs), health records



The Significance of Backing Up Salesforce

Considering your responsibility in managing your organizations' critical data on Salesforce, ensuring the protection and security of this information is paramount. The following points highlight key factors that emphasize the need for Salesforce backup and recovery.

Unintentional Data Deletion

Crucial records can be inadvertently deleted by system users, leading to the erasure of vital information from the system. To mitigate the impact of accidental deletions — whether caused by unintentional record removal, over-privileged users, metadata corruptions, or other factors – regular backups are essential for swift recovery and preventing data loss.

Data Integrity and Recovery

Data corruption can occur due to multiple factors, like system errors and network issues. Whether it's a result of human error, integration error, or unforeseen circumstances, maintaining reliable backups ensures that businesses can quickly recover and maintain data integrity. This proactive approach not only safeguards data against potential corruption, but also supports data consistency, compliance, and overall business resilience within the Salesforce environment.

Cybersecurity Threats

Malicious actors may attempt to compromise your data's confidentiality or integrity through tactics such as ransomware, phishing, or other cyberattacks. Ransomware, for instance, has the potential to access and delete your data, and then demand a ransom for data restoration. Attackers may also exploit vulnerabilities to compromise user credentials, which exposes the risk of data breaches or unauthorized data and storage access.

Compliance Requirements

Numerous businesses function within industries that have distinct requirements concerning data retention and compliance, such as healthcare and financial services. Failure to comply with these regulations can lead to legal complications and regulatory penalties.

Don't Depend on the Recycle Bin as Backup

The Salesforce Recycle Bin is a temporary storage area that holds records and data that have been deleted by users. While it can be a useful feature for recovering accidentally deleted items, it is not designed as a long-term data protection solution. The recycle bin only retains deleted records for a limited period (15 days by default) and does not retain metadata. After this period, the data is permanently deleted and cannot be recovered.
The recycle bin also has storage limits, and once those limits are reached, older items are automatically purged, even before the 15-day retention period is up.

Design your Data Protection Strategy

To create an effective backup and recovery strategy for Salesforce, you need to answer key questions that help define your organization's data protection needs, and the tools required to meet them. Here are some crucial considerations:

What Specific Salesforce Data Needs to Be Backed Up?

Consider whether to back up all data or just critical objects (e.g., accounts, contacts, opportunities, etc.) and records. Determine if custom objects, content documents, or metadata should be included in the backup.

How Will you Handle Salesforce Data Schema and Customizations?

Ensure that your strategy includes backing up custom fields, triggers, workflows, and other configurations in addition to standard data. Losing customizations can disrupt business operations even if the core data is preserved.

How Will you Ensure Data Integrity and Consistency During Backups?

Determine how your backup solution will ensure that data remains consistent, especially in multi-object relationships. Consider using tools that support full transactional consistency, so data is restored correctly after an outage.

Do You Need to Granularly Restore Data, and If So, are You Able To?

Safeguard your data by making sure you can easily search, compare and restore data and metadata quickly while keeping hierarchies intact.

How Will you Utilize Data Seeding and Data Masking?

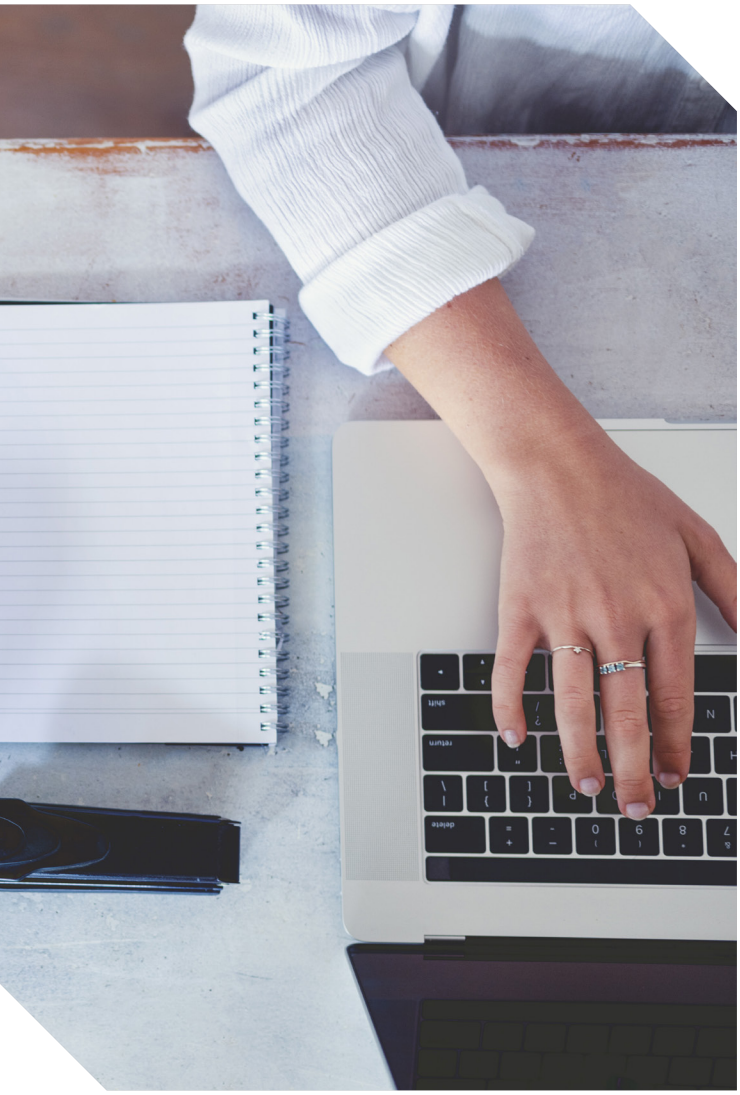
Enhance security by allowing teams to work with realistic data sets without exposing sensitive information. These tools also ensure compliance with regulations, mitigate risks in the event of data breaches, and facilitate collaboration while optimizing performance during development and testing.

What is Your Process for Testing Backup and Recovery Procedures?

Regularly test your backup and recovery process to ensure its functioning as expected and can restore Salesforce data in a timely and complete manner. Testing should be part of your overall disaster recovery (DR) plan.

How Will you Handle Large Data Volumes and Storage Costs?

Consider how your backup solution will scale with growing data volumes in Salesforce, and if the solution in question offers storage options that meet your budget and compliance needs.



What is Your Data Access and Encryption Policy for Backup Data?

Ensure that your backup data is securely stored and encrypted both in-transit and at-rest, and that only authorized personnel have access to it. Compliance with regulations such as GDPR, HIPAA, etc., is critical for protecting sensitive customer information.

How Long Should Salesforce Backup Data be Retained?

Retention requirements are often driven by corporate policies and regulatory compliance, which determine where, when, and how long Salesforce data can be stored.

Does Your Organization Use Other Platforms, and How are Those Being Protected?

It's likely that Salesforce is one of many SaaS solutions your organization employs, alongside other cloud-based and on-premises platforms, all of which need to be protected. Consolidating and standardizing data protection is strongly advised to eliminate the complexity of multiple point products from multiple vendors.

These factors will vary depending on the criticality of your Salesforce data and applications, as well as the governance and compliance requirements that surround it.

Security

Security is critical when it comes to Salesforce data, as it holds valuable business information and customer data that's essential to an organization's operations.

One of the key risks to security is human error, whether through accidental data exposure, improper access control configurations, or mistakes during updates. Employees may unknowingly provide inappropriate permissions or fall victim to phishing scams as well, which can compromise sensitive data. Therefore, it's crucial to implement strict RBAC, user training programs, and logging to monitor user activities, which minimizes the risk of human error that could lead to data breaches or unintentional data loss.

Equally important is defending against malicious attacks, such as hacking, data theft, or ransomware. Cybercriminals target platforms like Salesforce due to the valuable data stored within them, making it essential to protect Salesforce against unauthorized access and exploitation. Salesforce provides several security features, including as encryption and two-factor authentication (2FA), to help protect data from external threats. Organizations should also monitor for suspicious activity and ensure that their security practices comply with industry standards and regulations. By employing a multi-layered security strategy, organizations can create a strong defense against both human error and malicious attacks, ensuring that Salesforce data remains secure and available to trusted users.

Compliance

Every organization has regulatory and corporate standards they must meet to remain compliant. These standards for data retention play a pivotal role in determining the duration for which backups are retained, with considerations such as data criticality, regulatory stipulations, and business requirements shaping these policies.

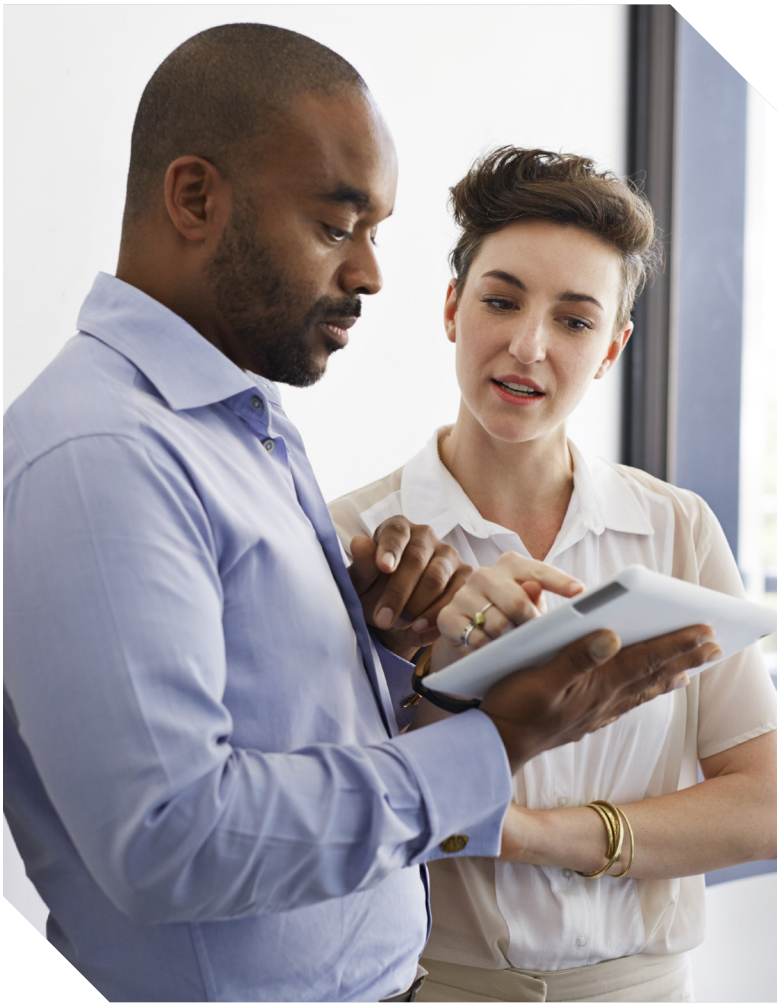
It is imperative for companies to regularly assess and revise their policies to ensure ongoing compliance and alignment with evolving business objectives. Defining specific data retention periods mitigates the risk of retaining excessive data, which could result in unnecessary cost or insufficient data, which may lead to compliance issues. This proactive approach ensures a balance that aligns with organizational needs and regulatory expectations. Some other necessary questions you should answer are:

What are the laws and regulations that govern how my company protects data?

- Digital Operations Resilience Act (DORA)
- General Data Protection Regulation (GDPR)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry (PCI)
- Health Insurance Portability and Accountability Act (HIPAA)

Are there any individuals in my organization that can help me identify regulations and achieve compliance? When is it safe and appropriate to delete data?

After understanding the compliance requirements, you can begin to appropriately design and automate policies to correctly manage the lifecycle of your data. Demonstrating compliance through reporting is also critical so you can operate in a state that is always audit-ready.



Archiving

Archiving in Salesforce is crucial for maintaining an efficient, secure, and cost-effective system. As data accumulates over time, it can impact system performance, increase storage costs, and complicate compliance efforts.

Archiving inactive or outdated data ensures that Salesforce runs smoothly by reducing unnecessary data load, while also providing a way to securely store and access historical information when needed. By implementing an effective archiving strategy, businesses can optimize their Salesforce environment, enhance compliance, and mitigate potential risks, ultimately supporting long-term success and scalability. There are many benefits to archiving both your Salesforce data and metadata, including:

- **Reduced storage costs:** By moving inactive data to cheaper storage solutions, organizations can cut down storage expenses.
- **Improved system performance:** Archiving less-critical data helps reduce the load on active databases, leading to faster query processing and better overall performance.
- **Enhanced compliance:** Archived data is securely stored and can be easily retrieved for regulatory requirements or audits.
- **Minimized risk surface:** Storing only necessary and active data reduces exposure to security breaches, which lowers the overall risk for sensitive information.

Granular Restore and Recovery

Not all data loss scenarios require a full system restore. Granular restore and recovery capabilities allow you to extract specific records or data elements. Make sure to use backup solutions or features that provide granularity to allow you to recover precisely what's needed in case of data loss or corruption.

This approach enhances efficiency, reduces downtime, and minimizes the impact of potential data issues by targeting and restoring only essential components which, in turn, ensures a more agile and responsive recovery process.

Beyond Salesforce data, prioritize the backup of metadata too. Metadata encompasses your organization's configuration, custom objects, fields, workflows, and more. Overlooking metadata backup can impede the restoration of your Salesforce instance to its previous working state. Metadata backups are also essential for maintaining the integrity of your system's configuration, data relationships, and compliance settings. This ensures that your Salesforce environment can be fully and accurately restored in the event of data loss or system issues, which aids in the continuity of business operations and data integrity.

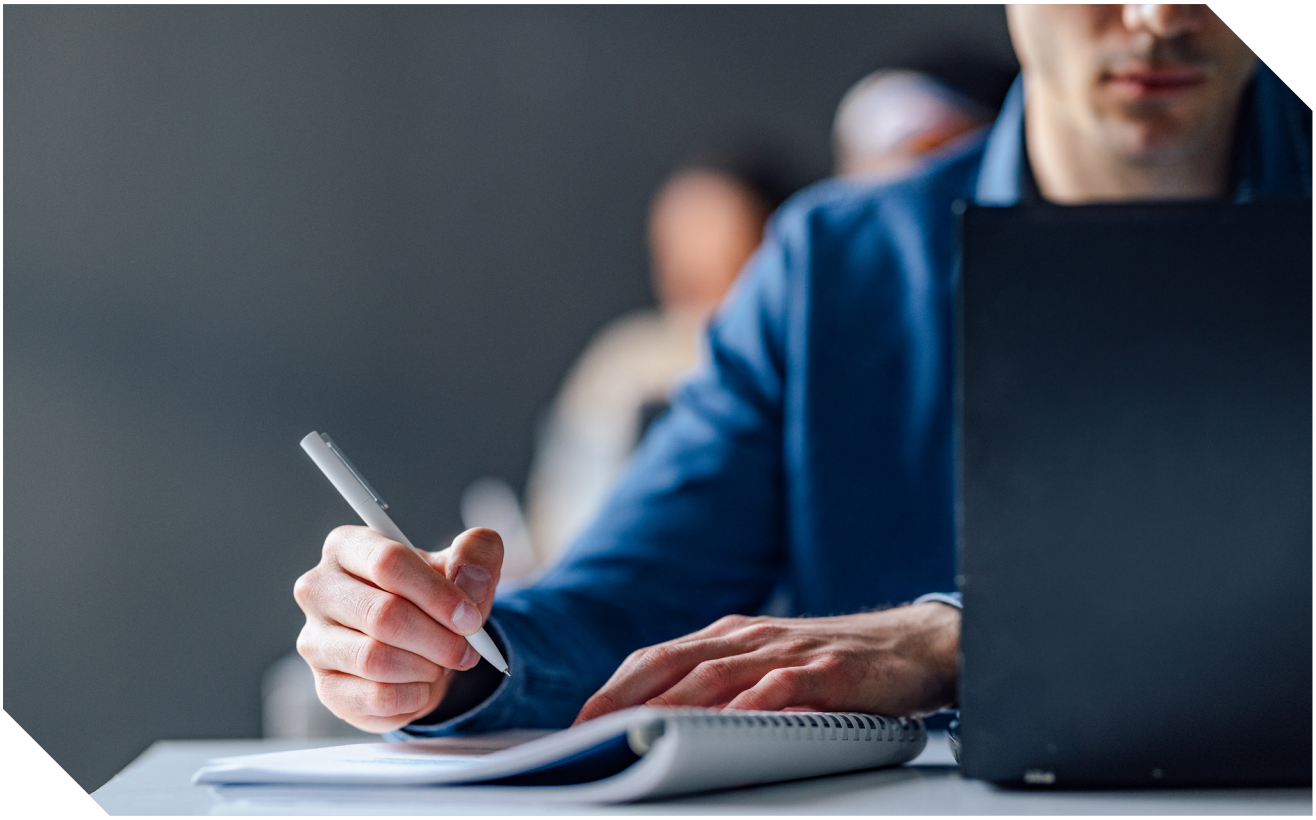
Documentation and Training

Once you have developed your Salesforce backup strategy, you will need to document it and train your team on it. Well-maintained documentation proves invaluable in both recovery drills and real data-loss scenarios, ensuring that recovery is swift and accurate.

This is key to enabling your team to adhere to standardized and effective procedures in the event of data loss. Therefore, it's important to clearly outline the steps involved in data and metadata backups, including schedules, automation settings, and any specific configurations.

This documentation guarantees consistent backup processes and serves as a guide for the IT team. Include details on how to test and verify backups, including procedures for data restoration. Regularly update this documentation to reflect any changes in your Salesforce environment or backup strategy.

Once you have completed documentation, you'll want to ensure that your team is proficient in using backup tools, executing recovery tasks, and following data recovery best practices. A well-trained team is better equipped to safeguard critical data, and providing training sessions on the initiation, monitoring, and testing of backups will help in the event restoration is needed. This knowledge empowers your team to respond effectively in the event of data loss, which enhances the overall reliability and success of your Salesforce backup strategy.



Monitoring and Testing

As threats and risks continually take on new forms, it is important that your Salesforce environment stays current. Testing your backups on a regular basis is crucial for ensuring their reliability.

Periodic data recovery tests ensure that your backup data can be successfully restored, which validates its integrity and usability for business operations. This proactive approach helps identify any issues in backup and restore procedures before they become critical during an actual data loss event. By regularly testing backups, you enhance confidence in your data recovery capabilities and ensure that your Salesforce backup strategy is reliable and effective.

In addition to testing, you should be monitoring your environment too. This is crucial for maintaining system integrity and ensuring smooth operations. Even small mistakes, such as incorrect data entries, misconfigured workflows, or overlooked automation errors, can quickly escalate into significant issues if not detected in time. Regular monitoring helps identify potential problems early, preventing disruptions in business processes, data integrity issues, or compliance risks. By staying vigilant and proactively addressing issues, you can safeguard your Salesforce environment from costly mistakes and ensure it continues to function efficiently and accurately.

Conclusion

Salesforce stands as an invaluable platform for businesses to efficiently manage and harness their critical data. The importance of Salesforce protection cannot be overstated, given the ever-present risk of data loss, security threats, compliance requirements, business continuity, and the need for seamless data migration.

In the constantly changing landscape of a data-driven world, proactive data protection emerges as a fundamental pillar for business resilience, growth, and long-term success. By implementing a comprehensive Salesforce backup strategy, adhering to the practices outlined above, and selecting a third-party solution, your business not only safeguards against existing threats, but is positioned to leverage data-driven opportunities in the future as well.

As an industry leader in data resilience, Veeam understands how important your data is to your organization. With Veeam Data Cloud, our single cloud platform that unifies resilience for all SaaS apps and data, your teams will have better management over their Salesforce environment while freeing up their time.

What's more, Veeam Data Cloud *for Salesforce* protects, secures, and restores critical data and metadata to keep your business running. Better yet, advanced data management and monitoring capabilities empower you to meet compliance confidently while lowering TCO. You will also be able to:

Eliminate downtime: Maintain productivity with automated, high-frequency backup, and precise, fast recoveries of data and dependencies.

Mitigate risks: Secure all your data while maintaining compliance through access control, encryption, and data masking.

Unlock value: Leverage archiving, unlimited storage, and sandbox seeding to lower TCO, all included in one predictable price.

Similar Content

6 Reasons for Microsoft Entra ID Backup

8 Benefits of a Backup Service for Microsoft 365

To see Veeam Data Cloud *for Salesforce* in action, schedule a demo with one of our specialists!