autorabit

A Step-by-Step Guide to Salesforce Data Security

An intentional and frequently updated approach to Salesforce data security provides continuous protection in the face of evolving threats and vulnerabilities.

Here are 8 steps you can take to improve the security of your Salesforce DevOps pipeline.

1 Understand Salesforce's Shared Responsibility Model

Salesforce is responsible for securing the infrastructure of the platform. Users are responsible for everything on top of that—including the data, customizations, third-party integrations, and applications developed on the platform.

2 Implement a Zero-Trust Strategy

Zero Trust is an approach to data security that recognizes threats can come from both inside and outside an organization.

3 Configure Profiles and Permission Sets

Customize profiles and permission sets to control which objects and fields users can access, as well as what actions they can perform on those objects.

4 Establish Access Controls

Additional layers of verification are critical to protect system data. Two-factor authentication must be utilized to add another layer of protection to your user accounts.

5 Leverage Field-Level Security

Field-level security restricts access to sensitive data fields within records and ensures that only authorized users can view or edit specific fields.

6 Schedule Repeated Audits of Permission Settings

Regular audits of these settings ensure your configurations are up-to-date and provide the coverage you need to maintain security and compliance with regulatory guidelines.

7 Stress the Importance of Best Practices

Clearly communicate best practices, encourage your team to ask questions to eliminate confusion, and give them everything they need to properly handle data.

8 Monitor Access Logs and Security Reports

Review access logs to verify each user within your Salesforce environment is a sanctioned employee.