13 Salesforce Security Best Practices to Implement Today

Wondering how to protect your cloud-based data from falling into the wrong hands? Following these Salesforce security best practices will allow you to leverage all of the platform's existing features to safeguard your company's and customers' data.

Getting Started:

- ☐ Use Salesforce's security Health Check to identify gaps in your org.

Salesforce Login Security:

- ☐ Tighten user password settings.
- ☐ Implement a company-wide sign-on policy.
  - ☐ Standardize user identity verification practices.
  - ☐ Implement My Domain and restrict logins to your new domain name.
- ☐ Optional: Restrict login hours for teams that never work off hours.
- ☐ Optional: Restrict login IP ranges for users that never work remotely.

Salesforce Object Security:

- ☐ Customize Salesforce object CRED settings for each user profile.

Salesforce Record Security:

- ☐ Restrict Salesforce org-wide sharing defaults.
- ☐ Build your role hierarchy to preserve access for managers and business leaders.
- ☐ Create custom sharing rules to give every user access to precisely what they need.

Salesforce Field Security:

- ☐ Restrict access to sensitive information by setting field-level security.
- ☐ Mask private data through Classic encryption or Shield Platform Encryption.

Salesforce Mobile Security:

- ☐ Optional: For mobile teams, customize Salesforce mobile app security settings.

Have any questions about the best way to tackle any of these to-dos?
Let us know if we can help!

torrent CONSULTING