ONE PAGE SUMMARY

IT & Software › Low Code / No Code › Security in Low Code

Introduction to Security in Low Code

Secure Your Low Code Applications Effectively!

DEFINITION

> Security in low code refers to the measures taken to protect applications built with minimal coding. It ensures data integrity, user privacy, and system reliability.

KEY CONCEPTS

Data Protection

Safeguarding sensitive information from unauthorized access or breaches.

User Authentication

Verifying user identities to ensure only authorized individuals can access applications.

Access Control

Setting permissions to determine who can view or modify application data.

Compliance Standards

Adhering to regulations like GDPR or HIPAA to protect user data.

Security Testing

Evaluating applications for vulnerabilities through various testing methods.

EXAMPLES

→ Implementing two-factor authentication for user login.

→ Encrypting data stored in the application database.

→ Regularly updating software to patch security vulnerabilities.

MEMORY TIPS

★ Remember 'D-U-A-C' for Data protection, User authentication, Access control, Compliance.

★ Think of a fortress: strong walls (data protection), guards (user authentication), and locked doors (access control).

★ Use the acronym 'SECURE' - Safety, Encryption, Compliance, User access, Regular updates, Evaluation.

COMMON MISTAKES

✗ Neglecting to update security protocols regularly.

✗ Overlooking user access levels, leading to unauthorized data access.

✗ Failing to conduct thorough security testing before deployment.

QUICK RECAP

Security in low code is essential for protecting applications and user data. Key aspects include data protection, user authentication, and compliance with standards. Regular testing and updates are crucial for maintaining security.