

ONE PAGE SUMMARY

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

Introduction to Security in Low Code

Understanding Security in Low Code Development

DEFINITION

Security in low code refers to protecting applications built with minimal coding. It ensures data integrity and user safety.

KEY CONCEPTS

Data Protection

Safeguarding sensitive information from unauthorized access and breaches.

User Authentication

Verifying the identity of users to ensure only authorized individuals access the system.

Access Control

Managing permissions to restrict what users can see and do within the application.

Compliance Standards

Following legal and regulatory requirements to protect user data and privacy.

Vulnerability Management

Identifying and addressing weaknesses in applications to prevent exploitation.

EXAMPLES

- Implementing multi-factor authentication for user logins.
- Regularly updating software to patch security vulnerabilities.
- Using encryption to protect sensitive data in transit.

MEMORY TIPS

- ★ Remember 'D-U-A-C-V' for Data, User, Access, Compliance, Vulnerability.
- ★ Think of a 'lock and key' for user authentication and access control.
- ★ Visualize a shield for data protection and compliance standards.

COMMON MISTAKES

- ✗ Neglecting regular software updates and patches.
- ✗ Overlooking user training on security best practices.
- ✗ Failing to implement proper access controls.

QUICK RECAP

Security in low code is vital for protecting applications and user data. Focus on data protection, user authentication, and compliance to ensure safe development practices.