

Security at the Core: Unraveling Secure by Design Principles

Secure by Design stands as a fundamental approach in building robust security from the ground up. These principles form the cornerstone of creating systems and products resilient to cyber threats.

Principles of Secure by Design:

Layered Defense: Implementing multiple layers of security measures to create a defense-in-depth strategy, preventing single-point failures.

Least Privilege: Providing minimal access rights necessary for tasks, reducing the potential impact of breaches or insider threats.

Default Secure Configurations: Employing secure default settings for systems or devices to prevent vulnerabilities right from installation.

Continuous Updates and Patching: Regularly updating software, firmware, and systems to address security flaws and vulnerabilities.

Data Minimization: Collecting and storing only necessary data, reducing the impact of breaches and protecting user privacy.

Resilience and Redundancy: Building systems resilient to failure, incorporating redundancy for critical functions to maintain operations.

Secure Authentication and Authorization: Implementing robust authentication methods and access controls to prevent unauthorized access.

User Awareness and Training: Educating users on security practices, fostering a security-conscious culture within organizations.

Monitoring and Incident Response: Proactive monitoring for anomalies and swift incident response to mitigate threats effectively.

Testing and Validation: Thoroughly testing systems and products for security vulnerabilities, ensuring robustness before deployment.

www.centextech.com

[Centex Technologies](#)



13355 Noel Road, Suite #1100
Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street,
Killeen, TX 76541

Phone: (254) 213 - 4740

1201 Peachtree ST NE,
400 Colony Square #200
Atlanta, GA 30361

Phone: (404) 994 - 5074

Capital Factory, 701 Brazos Street,
Suite 500 Austin, TX 78701

Phone: (512) 956 - 5454