

SECURITY TESTING CHECKLIST

prevention

TECHNOLOGY

- Make software updates mandatory
- Implement single-sign-on (SSO)
- Review authentication and access procedures
- Remove sensitive data and secrets from code
- Implement encryption protocols
- Apply secure coding practices
- Integrate security testing into the development lifecycle
- Pentest applications, APIs, and mobile apps
- Secure internet and Wi-Fi settings
- Install and configure firewalls and endpoint protection
- Monitor for suspicious activity in systems and networks
- Set up logging and monitoring
- Secure remote access (VPN, MFA, device checks)
- Perform regular network penetration tests
- Back up data and test recovery
- Stay up to date about new vulnerabilities
- Perform continuous vulnerability management

ORGANIZATION

- Appoint a security officer (CISO or equivalent)
- Create a security incident response plan and procedures
- Assess security risks of suppliers and third parties
- Align with security frameworks (ISO 27001, NIS2, CIS Controls)
- Review and improve security annually at management level
- Set up centralized logging and monitoring
- Ensure proper joiner-mover-leaver processes

PEOPLE

- List all employees and match with hardware (Asset Management)
- Organize phishing simulations
- Provide security training and awareness for all staff
- Use a password manager and enforce strong passwords
- Implement multi-factor authentication (MFA)
- Apply the principle of least privilege