Systems Design, Build, and Implementation Standard

Table of contents

Change History 2
1. Purpose, scope, and Users 5
2. Compliance and exceptions 5
3. Objectives 5
4. Security requirements of information systems 6
    4.1 Securing application services on public networks 6
    4.2 Protecting application services transactions 7
5. Secure development standards 7
6. Software development lifecycle (SDLC) 8
    6.1 Concept and planning 9
    6.2 Requirements and design 9
    6.3 Development and implementation 10
    6.4 Testing and verification 10
    6.5 Deployment and release 11
    6.6 Operations and maintenance 12
    6.7 End of Life and decommissioning 13
7. Secure coding 13
    7.1 Secure coding training for developers 13
    7.2 Secure coding techniques 13
    7.3 Source code control 20
    7.4 Hardcoded credentials, tokens, and other secrets 20
    7.5 Development 20
    7.6 Testing 21
        7.6.1 Release testing 22
    7.7 Pre-Production 23
    7.8 Deployment 23
8. Secure design principles 24
    8.1 Defense in depth 24
    8.2 Fail safe 25
    8.3 Least privilege 25
    8.4 Separation of duties 25
    8.5 Economy of mechanism 26

8.6 Complete mediation 26
8.7 Least common mechanism 26
8.8 Leveraging existing components 27
9. Secure system engineering 27
9.1 Secure development environment 27
9.1.1 Separation of development and operational environments 28
9.1.2 Development within a sandbox 28
9.1.3 Testing within a sandbox 29
9.2 Outsourced development 30
9.3 System security testing 30
9.4 System acceptance testing 30
9.5 Deployment 31
9.6 Technical review of applications after operating platform changes 31
9.7 Restrictions on changes to software packages 32
10. Vulnerability remediation 32
10.1 Exceptions 33
11. Roles and responsibilities pertaining to this Standard 33
12. Definitions 37
13. Related documents 40
14. Validity and standard management 40