



# Technical Security Standard



## Table of contents

Change History	2
1. Purpose, scope, and Users	7
2. Compliance and exceptions	7
3. Objectives	8
4. Access control	8
4.1 Access classification	8
4.2 Role Based Access Control (RBAC)	9
4.3 User access provisioning	9
4.4 Review of access rights	10
4.5 Removal or adjustment of access rights	10
4.6 Privileged access rights	11
4.7 System and application access	12
4.8 Privileged utility program access	12
4.9 Program source code access	13
4.10 Segregation of duties	13
4.11 Secure log-on procedures	14
4.12 Remote access	15
5. Identity management	16
5.1 Authentication information management	17
5.2 Password management	17
5.2.1 User passwords	18
5.2.2 Application service account passwords	19
5.3 Multi-Factor Authentication (MFA)	19
6. System and information integrity	19
6.1 Data protection	20
6.1.1 Data masking	20
6.2 Malware protection	21
6.3 Web filtering	22
6.4 Anti-Virus	22
6.5 Encryption	22
6.5.1 Key management	24
6.6 Email and web browser protections	25
7. Virtual environments and shared resources	26



8. Remote work	27
9. Backup and restore	27
10. Information flow control	27
10.1 Boundary protection and data transfers	28
10.2 Role-Based and Attribute-Based Access Controls (RBAC & ABAC)	28
10.3 Logging and monitoring	28
11. Data Loss Prevention and content inspection	29
12. Vulnerability management	29
12.1 Penetration testing	31
12.1.1 Retention period	31
12.1.3 Business Unit requirements	31
12.2 Security Assessments	31
12.3 Vulnerability scanning	31
12.3.1 Objectives	32
12.4 Patch management	33
12.4.1 Hardware and software requirements	33
12.4.2 Patch deployment	33
12.4.3 Severity ratings	34
12.4.4 Patch identification process	34
12.4.5 Patching schedule priority matrix	34
12.4.6 Risk assessment	35
12.4.7 Patch acceptance and deployment	35
12.4.8 Exceptions	36
13. Network security	36
13.1 Network segmentation and security zones	36
13.2 Boundary defense	38
13.3 Voice over Internet Protocol	39
13.4 Internal network connections	39
13.5 External network connections	39
13.6 Limitation and control of network ports, protocols, and services	40
13.7 Securing the Domain Name System	40
13.8 Wireless security	40
14. Incident reporting	41
15. Roles and responsibilities pertaining to this Standard	41
16. Definitions	42



17. Related documents	45
18. Validity and standard management	46