



Physical and Environmental Protection Standard



Table of contents

Change History	2
1. Purpose, scope and Users	5
2. Compliance and exceptions	5
3. Objectives	6
4. Site security classification	6
5. Secure areas	6
5.1 Physical security perimeter	6
5.1.1 Building construction	6
5.1.2 Entrance locations	7
5.1.3 Perimeter lighting	7
5.1.4 Perimeter fencing	7
5.1.5 No trespassing	7
5.1.6 Emergency exit / Fire doors	7
5.1.7 Delivery and loading areas	8
5.2 Physical entry controls	8
5.2.1 Visitors	8
5.2.2 Court & process servers and law enforcement interactions	8
5.2.3 Access audits	8
5.2.4 Access Badge/Fob requirements	9
5.2.5 Fob credentials	9
5.2.6 Key control	9
5.2.7 Confidential areas	9
5.3 Securing offices, rooms, and facilities	9
5.3.1 Data rooms	10
5.4 Physical security monitoring	10
5.5 Protecting against external and environmental threats	10
5.6 Working in secure areas	10
6. Equipment	11
6.1 Equipment siting and protection	11
6.2 Supporting utilities	11
6.3 Cabling security	12
6.4 Equipment maintenance	12
6.5 Removal of assets	12
6.6 Security of equipment and assets off-premises	13



6.6.1 Authorization	13
6.6.2 Best practices	13
6.7 Secure disposal or reuse of equipment	13
6.8 Unattended user equipment	13
7. Management of media	13
7.1 Approved sanitization and disposal techniques	15
7.1.1 Overwriting of electronic media	15
7.1.2 Degaussing electronic media	15
7.1.3 Physical destruction of media by shredding	15
7.1.4 Physical destruction of electronic media using a third party service	16
7.1.5 Cryptographic Erase prior to sanitization	16
7.1.6 Authorized use of Cryptographic Erase	16
7.1.7 Verification of sanitization results	17
7.1.8 Certificate of sanitization	17
8. Clear desk and clear screen policy	18
8.1 Clear desks	18
8.2 Clear screens	18
8.3 Locked screens	18
9. Environmental protection	19
10. Incident reporting	19
11. Roles and responsibilities pertaining to this Standard	20
12. Definitions	21
13. Related documents	22
14. Validity and standard management	22