

Inhaltsverzeichnis

1.	DV-Szenario und Begriffe	1
1.1	Individuelle Datenverarbeitung (IDV)	1
1.2	Arbeitsplatzcomputer	1
1.3	APC-Nutzungsspektrum	4
1.4	Betriebssysteme	5
1.4.1	MS-DOS bzw. PC-DOS	5
1.4.2	OS/2	8
1.4.3	UNIX und UNIX-Derivate	9
1.5	Einsatzvoraussetzungen	13
1.6	Abhängigkeiten	13
1.7	Datensicherung	14
1.8	Datenschutz	15
1.9	Rechtsvorschriften zur Datenverarbeitung	16
2.	Personelle Anforderungen	17
2.1	Benutzerservice	17
2.1.1	Allgemeine Aufgabenbeschreibung	17
2.1.2	Systemverwaltung, -pflege und -kontrolle	18
2.1.3	Hardware-Kataster	18
2.1.4	Software-Kataster	19
2.1.5	Verfahrensentwicklung, -pflege und -dokumentation	21
2.1.6	Verfahrenstest und -freigabe	21
2.1.7	Benutzeranweisung APC	21
2.1.8	Copyright/Urheberrechtsschutz von Software	22
2.1.9	Verwendung privater APC	22
2.1.10	Verwendung privater Software	22
2.1.11	Verwendung von Laptops	23
2.2	Aufgaben des Datenschutzbeauftragten	23
2.3	Aus- und Fortbildung der Benutzer	25
2.4	Verpflichtung	25
3.	Installationsanforderungen	27
3.1	Aufstellungsort des Arbeitsplatzcomputers	27
3.2	Intrusionsschutz	29
3.3	Zutrittsberechtigung	31
3.4	Vernetzung / Verkabelung / DFÜ-Anschluß	32
3.5	Kompromittierende Abstrahlung	33

3.6	Umweltverträglichkeit	35
3.7	Recycling und Sanierung von Elektronikgeräten	36
4.	Betrieb des Arbeitsplatzrechners	38
4.1	Unkontrolliertes Ausschalten des Gerätes	39
4.2	Systemgenerierung	39
4.3	Systemverwaltung	40
4.4	Benutzerverwaltung	40
4.5	Zugriffssicherung	41
4.6	Paßwortverwendung	42
4.6.1	Grundsätze	42
4.6.2	Verwaltung von Paßwörtern	43
4.6.3	Verwendung von Paßwörtern	44
4.7	Programmierung und Freigabeverfahren	44
4.8	Wartung durch den Hersteller	45
4.8.1	Maßnahmen der Zugangskontrolle	46
4.8.2	Organisation der Datenträgerkontrolle	46
4.8.3	Maßnahmen zur Speicherkontrolle	47
4.8.4	Maßnahmen zur Zugriffskontrolle	47
4.8.5	Maßnahmen zur ordnungsgemäßen Durchführung der Wartung	47
4.8.6	Maßnahmen zur Transportkontrolle	48
4.9	Datenträger	48
4.9.1	Handhabung von Datenträgern	49
4.9.2	Bereitstellung von Datenträgern	50
4.9.3	Schreibschutz	50
4.9.4	Datenträgerinventur	50
4.9.5	Warnung vor Killerdisketten	50
4.9.6	Vorsicht bei Demo-Disketten	51
4.9.7	Festplattenreorganisation	51
4.9.8	Entsorgung von Datenträgern	51
4.10	Datensicherung und Datenträgerverwaltung	52
4.10.1	Datenträgerverwaltungssystem	54
4.10.2	Datensicherheitsfunktionen	54
4.10.3	Organisation der Datensicherung	55
4.10.4	Zentrale Datensicherung	57
4.10.5	Aufbewahrung der Sicherungsbestände	57
4.10.6	Rekonstruktion von Datenbeständen	57
4.10.7	Verschlüsselung	58
4.10.8	Datenträgeraustausch	59
4.11	Aufzeichnung von Ablaufdaten	60
4.11.1	Anforderungen an das Protokollsystem	60
4.11.2	Aufbau der Protokollsätze	61
4.11.3	Berichtsmerkmale und Audit-Programme	61

4.11.4	Sicherheitsbericht	62
4.12	Reaktion des Systems auf Fehlverhalten oder Mißbrauchsversuche der Benutzer	62
5.	Sicherheitsgrundsätze bei unterschiedlichen Einsatzformen einschließlich Vernetzung	63
5.1	Stand-alone-Betrieb	63
5.1.1	Diskettenbetrieb	64
5.1.2	Festplattenbetrieb	64
5.1.3	Zugriffs- und Benutzerkontrolle	65
5.1.4	Revisionsfähigkeit	66
5.1.5	Elementare Sicherheitsmaßnahmen	66
5.1.5.1	Single-User-Betrieb	66
5.1.5.2	Multi-User-Betrieb	67
5.2	Vernetzte Systeme	67
5.2.1	Hardware	69
5.2.1.1	Netzwerktopologien	69
5.2.1.2	Physikalische Eigenschaften	71
5.2.2	Netzwerkbetriebssystem	72
5.2.3	APC-Netz	73
5.2.4	Netzadministration	75
5.2.5	Netzwerk-Server	77
5.2.6	Anschluß an einen Host	78
5.2.6.1	Stationsidentifizierung	79
5.2.6.2	Zugriffsberechtigung	79
5.2.6.3	File Transfer	79
5.2.6.4	Elementare Sicherheitsmaßnahmen	81
5.2.7	Anschluß an ein beliebiges System	82
5.3	Sicherung von Leitungen und Anschlüssen	82
5.4	Ein Beispiel: das Sicherheitssystem von NetWare 386	83
5.4.1	Zugangssicherheit	83
5.4.2	Zugriffssicherheit	84
6.	Computerviren	87
6.1	Aufbau eines Virus und Virusarten	88
6.2	Virusähnliche Programme	90
6.3	Infektionsquellen	90
6.4	Sicherheitsmaßnahmen	91
6.5	Spezielle Programme gegen Viren	92
6.6	Maßnahmen bei Virenbefall	94
6.7	Frühwarnsysteme	94
6.8	Versicherungsschutz	95
6.9	Anti-Viren-Kreis	95

7.	Computerkriminalität	97
7.1	Computerbetrug	99
7.2	Computerspionage	99
7.3	Computersabotage	100
7.4	Computermißbrauch	100
7.5	Ursachen für Computerkriminalitätsfälle durch Outsider	100
7.6	Straftatbestände bei Computerkriminalität	101
7.6.1	Strafgesetzbuch (StGB)	101
7.6.2	Gesetz gegen den unlauteren Wettbewerb (UWG)	101
7.6.3	Urheberrechtsgesetz (UrhG)	101
7.7	Schutzmaßnahmen vor Computerkriminalität	102
7.8	Vorsicht bei Sonderangeboten	102
8.	Notfall- und Katastrophenvorsorge	104
8.1	Katastrophenhandbuch	104
8.2	Ressourcen	105
8.2.1	Hardware	105
8.2.2	Software	105
8.2.3	Datenbestände	106
8.2.4	Ausweichraum für Neuinstallation des Arbeitsplatzrechners	106
8.2.5	Dokumentation	106
8.3	Entscheidungskriterien für eine Backup-Lösung	107
9.	Versicherungsschutz	108
9.1	Hardware	108
9.2	Datenträger	109
9.3	Ausfallfolgeschäden	109
9.4	Computerkriminalität und Datenmißbrauch	110
10.	Zusätzliche Sicherheitseinrichtungen	112
10.1	Datensicherungsschränke	112
10.2	Sicherung der Stromversorgung	113
10.2.1	Überspannungsschutz und unterbrechungsfreie Stromversorgung (USV)	113
10.2.2	Statische Aufladung	115
10.3	Mechanische Sicherheitseinrichtungen	116
10.3.1	PC-Schlösser	116
10.3.2	Kennzeichnung von Datenträgern	116
10.3.3	Türsicherung	116
10.3.4	Datenträgervernichtung	116

11.	Die zehn Kontrollbereiche der APC-Sicherheit	118
11.1	Zugangskontrolle	118
11.2	Datenträgerkontrolle	118
11.3	Speicherkontrolle	119
11.4	Benutzerkontrolle	119
11.5	Zugriffskontrolle	120
11.6	Übermittlungskontrolle	120
11.7	Eingabekontrolle	121
11.8	Auftragskontrolle	121
11.9	Transportkontrolle	121
11.10	Organisationskontrolle	122
12.	Sicherheitsprodukte	123
12.1	Beispiele	123
12.2	Zertifizierung von DV-Komponenten	124
12.3	Sicherheitsfunktionen	125
 Anhang		
13.	Zusammenstellung von Sicherheitsprodukten	127
13.1	Softwareprodukte	127
13.2	Hardwareprodukte	160
13.3	Kombinierte Hard- und Softwareprodukte	165
13.4	Sicherheits-APC	173
13.5	Sonstige Sicherheitskomponenten	175
13.6	Sicherheitsnormen	178
13.7	Formulare	182
13.7.1	Hardware-Kataster	182
13.7.2	Software-Kataster	183
13.7.3	User-Kataster	184
13.7.4	Datenträger-Kataster	185
13.7.5	Störungslögbuch	186
13.7.6	Verpflichtungserklärung	187
14.	Literaturhinweise	188
15.	Glossar	190
16.	Stichwortverzeichnis	203