

Innehåll

Introduktion.....	6	4 Kringmiljö	100
1 Säkerhetsledning och organisation	22	1 Yttre miljö	100
1 Ledning	22	2 Inre miljö	103
2 Organisation.....	26	5 Tillträde.....	106
3 Ansvar.....	29	1 Mekaniska och teletekniska tillträdes-	
4 Utbildning/medvetenhet	31	mekanismer	106
5 Central BKS-administration.....	33	2 Behörighet till lokaler.....	108
6 Ekonomiskt skydd	34	3 Säkerhetsanpassning	110
7 Legala krav	36	6 Försörjning	112
8 Interna regler och avtal	38	1 Klimat.....	112
9 Hantering av utrustning.....	41	2 Kraftförsörjning.....	115
10 Incidenthantering	42	3 El-miljö	116
11 Projektering/anskaffning	45	4 Service och underhåll av fysiska komponenter..	118
12 Kontroll.....	46	7 Brandskydd	122
13 Hantering av tekniska sårbarheter	47	1 Planering.....	122
14 Identifiering av risker med utomstående parter....	49	2 Brandsektionering.....	124
15 Hantering av säkerhet vid kundkontakter.....	52	3 Utformning	125
16 Hantering av säkerhet i tredje partsavtal	55	4 Brandbelastning.....	127
17 Förteckning över tillgångar.....	60	5 Brandlarm	129
18 Ägarskap för tillgångar	61	6 Brandsläckningsutrustning.....	131
19 Godtagbar användning av tillgångar	62	8 Skydd mot vattenskador.....	134
2 Personal	64	1 Utformning	134
1 Inför anställning.....	64	2 Larm.....	136
2 Under anställning	66	9 Systemsäkerhet.....	138
3 Ansvar vid upphörande eller ändring av		1 Behörighetskontroll – Införande	138
anställning.....	67	2 Behörighetskontroll – Organisation.....	140
4 Nyckelbefattningar/personer	68	3 Behörighetskontroll – Uppdatering.....	142
5 Behörighet	69	4 Behörighetskontroll – Styråtgärder	143
6 Kompetens.....	71	5 Behörighetskontroll – Uppföljning	145
7 Utnyttjande av konsulter mm.....	72	6 Behörighetskontroll – Identifiering.....	147
3 Tillgänglighet/tillförlitlighet	76	7 Behörighetskontroll – Åtkomstkontroll.....	150
1 Driftstörningar	76	8 Behörighetskontroll – Rapportering/Analys	152
2 Svarstider.....	78	9 Behörighetskontroll – Krypteringspolicy.....	154
3 Belastning	79	10 Behörighetskontroll – Nyckelhantering	156
4 Planering för löpande produktion.....	80	11 Operativsystem – Införande.....	159
5 Kommande produktion	82	12 Operativsystem – Åtkomst	161
6 Användning av system.....	83	13 Operativsystem – Förändring.....	163
7 Underhåll.....	84	14 Operativsystem – Virus/skadliga program	164
8 Säkerhetsåtgärder mot skadlig kod.....	85	15 Operativsystem – Användandet av system/ program.....	165
9 Validering av indata.....	88	16 Operativsystem – Applikationer	166
10 Styrning av intern bearbetning.....	90	17 Operativsystem – Databaser	167
11 Meddelandeintegritet	92	18 Loggfunktion – Loggning.....	169
12 Validering av utdata	93	20 Underhåll – Service	173
13 Tjänsteleverans.....	94		
14 Övervakning och granskning av tjänster från tredje part	95		
15 Ändringshantering av tjänster från tredje part.....	98		

10 Nätverk/telekommunikation	176	14 Kontinuitetsskydd	232
1 Nätadministration – Felhantering	176	1 Planering.....	232
2 Nätadministration – Dokumentation	178	2 Förvaltning	235
4 Nätadministration – Avbrottsplanering och redundans	181	3 Affärsberoendesanalys (Business Impact Assessment – BIA).....	237
5 Behörighet – Identifiering	183	4 Reservlösningar	238
6 Behörighet – Åtkomst.....	184	5 Krisledning och krishantering.....	240
7 Skydd vid överföring – Fysiskt skydd.....	187	6 Plan för återställande	243
8 Skydd vid överföring – Skydd mot obehörig uppkoppling.....	188	7 Planering för återgång till normal drift.....	246
9 Skydd vid överföring – Skydd mot avlyssning och förändring.....	190	8 Underhåll och distribution av planen	248
10 Koppling till Internet – Brandvägg (Firewall)	191	9 Utbildning.....	250
11 Användning av e-tjänster – Säkerhet.....	193	10 Övning och test	253
11 Systemutveckling/Systemändringar	196	11 Uppföljning/kontroll	259
1 Projektering/anskaffning	196	15 Underlag inför en analys	262
2 Programmering	198	1 Underlag som sänds ut före en Gap-analys	262
3 Utvecklingsmiljö	199	2 Underlag inför en Gap-analys – enkäten	264
4 Test	200	16 Underlag efter en analys.....	272
5 Dokumentation.....	201	1 Underlag som sänds ut efter en Gap-analys	272
6 Säkerhetsaspekter	203	17 Underlag efter en analys – slutrapport med åtgärdsplan.....	282
7 Driftsättning.....	205	1 Underlag som sänds ut när rapporten är klar	282
8 Change management/ändringsrutiner	206	Gap-analys.....	283
12 Persondatorer/arbetsstationer	208	Bakgrund.....	284
1 Ansvar	208	Resultat från Gap-analysen	285
2 Behörighet	209		
3 Funktion	210		
4 Säkerhetskopiering	212		
5 Virus/skadliga program	213		
6 Säkerhetsskydd för utrustning utanför verksamheten	215		
7 Distansarbete.....	216		
13 Säkerhetskopiering/arkivering.....	218		
1 IT-produktions kopiering av aktivt data.....	218		
2 Informationsbehandling – Arkivering av filer	222		
3 Verksamhetsenheter – Magnetiska media	223		
4 Verksamheten – Pappersdokument.....	225		
5 Förvaring.....	226		
6 Transport.....	228		
7 Hantering	228		