Bilaga 10

1 Risk- och sårbarhetsanalys

I detta kapitel utgår vi från identifierade riskscenarier i följande bilagor:

- Bilaga X – Informationsklassning, digitalt stöd i hemmet.xls

Vi värderar hur stor sannolikheten är för att en risk ska inträffa samt bedömer konsekvensen av om risken inträffar. Vi använder oss av nedanstående skalor.

Skalan för sannolikheten är följande:

Värde	Benämning	Innebörd/betydelse
4	Ofta	Kan inträffa månadsvis
3	Regelbundet	Kan inträffa kvartalsvis
2	Sällan	Kan inträffa årligen
1	Mycket sällan	Inträffar någon gång var fjärde år, jmf mandatperiod

Skalan för konsekvens är följande:

Värde	Benämning	Innebörd/betydelse
4	Allvarlig	Data är permanent borta, allvarlig personskada eller dödsfall, betydande ekonomisk skada, mycket stor kränkning, röjning av känsliga personuppgifter och liknande.
3	Betydande	Ekonomisk skada, risk för betydande personskada kränkning, röjning av personuppgifter och likande.
2	Måttlig	Måttlig påverkan på verksamheten, risk för måttlig personskada
1	Försumbar	Försumbar påverkan, ingen kränkning

Riskvärdet (RV) beräknas som:

- Värdet av sannolikheten gånger konsekvensen
  - Högsta riskvärdet kan bli 16 (4x4) och ska prioriteras
  - Lägsta riskvärdet kan bli 1 (1x1) och är i stort sett försumbart

Identifierade risker i grafisk form

Sannolikhet					
	4		R11, R38,	R13, R15, R17, R21, R22, R39, R51, R52, R55	R19, R20, R44, R48, R49,
	3		R28, R29, R36, R56	R5, R12, R23, R26, R37, R46, R53,	R32, R34, R35, R42, R43, R47,
	2		R2, R4, R14	R7, R8, R30, R31, R40, R41, R50,	R27, R45, R54,
	1		R3, R18	R1, R9, R16, R25, R33,	R6, R10, R24,
		1	2	3	4
		Konsekvens			

Varje enskild risk kommenteras i åtgärdsplanen, bilaga 7. Riskerna är numrerade med hänvisning till källan, dvs till aktuell bilaga och kapitel. Till detta anges ett Risknummer R1, R2 osv. (Rnr=Risknummer). Detta för att åstadkomma en följsamhet genom hela analysen, där varje enskild risk och händelse kan följas upp från identifierad risk till åtgärd av risk.

Rnr	ID nr	Risken att	på grund av	S	K	RV
R1	IK 4	en SÄ saknas	rollen inte är utsedd	1	3	3
R2	IK 5	systemet underhålls felaktigt	inaktuell förvaltningsmodell	2	2	4
R3	IK 6	ansvar för personuppgifterna hanteras oaktsamt	rollen PuO inte är utsedd	1	2	2
R4	IK 7	systemet införs utan full kontroll	kunskapsnivån inte är säkerställd hos de ansvariga	2	2	4
R5	IK 30	känslig information röjs på mobil enhet	relevanta säkerhetskrav inte är införda	3	3	9
R6	IK 43	otillbörlig användning av personuppgifter sker	leverantör och kund har olika uppfattningar gällande ansvar	1	4	4
R7	IK 49	att ett larm hanteras fel, t.ex pausar	bristande kompetens	2	3	6
R8	IK 50	utbildning uteblir	utbildningsplan saknas	2	3	6
R9	IK 51	ansvar inte kan tilldelas person som utför felaktig handling	rutin för detta saknas	1	3	3
R10	IK 54	tillgångar som hw och sw inte supportas längre	support utgått och det inte framgår i förteckningar att tillgångarna finns kvar	1	4	4
R11	IK 55	tillgångar sprids försvinner (kastas t.ex.)	rutin saknas för återlämning	4	2	8
R12	IK 56	vi upprättar felaktiga (ej optimala) rutiner	bristande insyn i driftdokumentation	3	3	9
R13	IK 57	handhavandefel sker	användardokumentation saknas	4	3	12
R14	IK 58	uppföljning inte sker på processer och rutiner	avsaknad av rutin, t.ex. förvaltingsplan, APT	2	2	2
R15	IK 60	användare gör fel	genomgång ej skett	4	3	12
R16	IK 70	klassning inte genomförs	avsaknad av förvaltningsplan	1	3	3
R17	IK 78	en incident inte anmäls (och följs upp)	rutin inte följs	4	3	12
R18	IK 95	behörigheter sätt supp utan SÄ godkännande		1	2	2
R19	IK 96	tillgång till system ges med enkelt åtkomst	bristande 2-faktor.	4	4	16
R20	IK 108	personal tillser en brukare otilbörligt	brister i tilldelning av rättigheter	4	4	16
R21	IK 112	en användare har felaktig åtkomst	felaktig behörighetstilldelning	4	3	12
R22	IK 115	se 112		4	3	12
R23	IK 116	att behörigheter röjs för anställd med höga behörigheter		3	3	9

Rnr	ID nr	Risken att	på grund av	S	K	RV
R24	IK 120	intrång sker	defaultlösenordet kvarstår	1	4	4
R25	IK 134	viktig lagstiftning inte följs	okunskap om de legala kraven	1	3	3
R26	IK 138	loggutdrag inte är möjliga	logg ej sparas / skapas	3	3	9
R27	IK 183	underhåll gör på tider som inte överensstämmer med verksamhetens krav	bistande rutiner för uppgraderingar	2	4	8
R28	IK 194	organisationen för systemförvaltning saknas		3	2	6
R29	IK 195	likartade incidenter upprepas	avsaknad av uppföljning	3	2	6
R30	IK 197	kommunen inte i alla situationer vet hur man ska agera	åtgärdsplaner saknas	2	3	6
R31	IK 200	kommunen är omdeveten av vissa risker	avsaknad av riskanalys	2	3	6
R32	IK 206	verksamhet blir onödigt drabbad	avsaknad av rutin för akutuppdateringar	3	4	12
R33	IK 207	systemet överbelastas	undermålig kapacitet	1	3	3
R34	IK 215	utbrott av skadlig kod sker	felaktiga säkerhetsuppdateringar	3	4	12
R35	IK 220	systemet inte kan återställas vid en ev krash eller att icke relevant data läses tillbaka	inga planerade TÅP tester utförst eller att gammal data läses tillbaka som inte är relevant.	3	4	12
R36	IK 222	logghanteringen är bristfällig		3	2	6
R37	IK 230	uppföljning av händelse försvåras	felaktiga tidsinställningar	3	3	9
R38	IK 242	systemet inte uppfyller kraven	överenskommelse inte tecknats	4	2	8
R39	IK 267	personuppgifter hanteras olagligt	brister i processerna	4	3	12
R40	IK 276	information används till annat än vad som var avsikten	brister i processerna	2	3	6
R41	IK 277	krypterad information läcker	brister i rutin vid dekryptyering och lagring	2	3	6
R42	IK 279	leverantören anser sig ha äganderätt till information i systemet		3	4	12
R43	IK 280	sekretessbelagd information kommer extern part till känna	brister i avtal	3	4	12

Rnr	ID nr	Risken att	på grund av	S	K	RV
R44	IK 291	testmiljö inte kan upprättas	svårigheter att simulera verklig miljö	4	4	16
R45	IK 292	osäker kod lagras i systemet, Se 215	svårigheter med validering av kod, (IoT)	2	4	8
R46	IK 299	verksamheten inte vet hur den ska agera då systemet ligger nere	felaktighet eller avsaknad av kontinuitetsplan	3	3	9
R47	IK 300	återställning misslyckas efter avbrott (se även 220)	felaktigheter i återställningsplan för drift	3	4	12
R48	IK 307	kommunen bryter mot PuL och nya direktivet	brister i insyn hos leverantör	4	4	16
R49	IK 308	sårbarheter inträffar	brister i testning	4	4	16
R50	IK 328	systemförvaltaren inte har tillräcklig kunskap om systemet (se även 206)	brister i rutin vid akutuppdateringar	2	3	6
R51	IK329	parterna inte vet vilka de ska kontakta vid incidenter	dessa inte är kända	4	3	12
R52	IK 331	systemförvaltaren inte har tillräcklig kunskap om systemet	brister i återkoppling av incidenter	4	3	12
R53	IK 335	systemet inte utvecklas (se kavalityetsuppföljning)	brister i återkoppling	3	3	9
R54	IK 337	sekretessbelagd information röjs vid incidenter	brister i rutin	2	4	8
R55	IK 342	aktiviteter under incident kan inte följas upp	loggning av händelser inte skett	4	3	12
R56	IK 343	de roller som borde vara med i uppföljingar inte medverkar	det är svårt att förstå innan vilka som ska vara med	3	2	6

2 Handlingsplan

Rnr	ID nr	Åtgärd	Ansvarig	Status
R1	IK 4	Utse systemägare	Bestäms vid upphandling	Ej påbörjat
R2	IK 5	Fastställ förvaltningsmodell	Systemägare	Ej påbörjat
R3	IK 6	Försumbart		
R4	IK 7	Se över process för införande		
R5	IK 30	Identifiera och verkställ nödvändiga säkerhetsinställningar för mobila enheter		
R6	IK 43	Försumbart		
R7	IK 49	Informera och utbilda		
R8	IK 50	Upprätta utbildningsplan		
R9	IK 51	Försumbart		
R10	IK 54	Försumbart		
R11	IK 55	Inför rutin för hantering och återanvändning av enheter		
R12	IK 56	Samråd med leverantör om rätt insyn i respektive organisation driftrutin		
R13	IK 57	Skapa och underhåll dokumentation till användare		
R14	IK 58	Inför förvaltningsplan		
R15	IK 60	Introducera användare i rätt omfattning		
R16	IK 70	Se till att klassning finns med i förvaltningsplan		
R17	IK 78	Se till att rutin finns för incidenthantering, anmälan, åtgärd, återkoppling		
R18	IK 95	Behörighetskontrollsystem med delegation på beslut och verkställande		
R19	IK 96	Inför stark autentisering där behov finns		
R20	IK 108	Se över behörighetskontrollsystem och loggningsrutiner		
R21	IK 112	Samma som R18		
R22	IK 115	Samma som R18		
R23	IK 116	Skapa rutin för personal med höga behörigheter		
R24	IK 120	Inför rutin där default lösen alltid byts		

Rnr	ID nr	Åtgärd	Ansvarig	Status
R25	IK 134	Utbilda, informera, ge stöd till och hänvisa till information kunskap och fakta gällande legala krav		
R26	IK 138	Fatta beslut om loggning		
R27	IK 183	Inför i samråd med verksamheten tidslucka för service och underhåll		
R28	IK 194	Upprätta systemförvaltningsmodell		
R29	IK 195	Inför förvaltningsplan, följ upp händelser, ge återkoppling		
R30	IK 197	Upprätta kontinuitetsplaner		
R31	IK 200	Genomför riskanalyser kontinuerligt		
R32	IK 206	Inför rutin för akutuppdateringar		
R33	IK 207	I förvaltningsplan, inför kapacitetsberäkningar och belastningsanalyser		
R34	IK 215	Säkerställ att skydd mot skadlig kod finns på samtliga relevanta enheter		
R35	IK 220	I förvaltningsplan, inför tester och återläsning etc.		
R36	IK 222	logghanteringen är bristfällig		
R37	IK 230	Om möjligt, försök att få enheterna att synkronisera tiden, genom ntp eller motsvarande		
R38	IK 242	Tydliggör i avtal vad som förväntas		
R39	IK 267	Genomför processkartläggning och beakta särskilt behandling av personuppgifter i dessa gentemot legala krav		
R40	IK 276	Samma som R39		
R41	IK 277	Säkerställ att krypterad information även skyddas vid dekryptering och lagring, så att hela kedjan skyddas		
R42	IK 279	Tydliggör vem som är informationsägare		
R43	IK 280	I avtalen, se till att ansvar för sekretess är tydligt		
R44	IK 291	Sätt upp en relevant testmiljö, simulera tester och utvärdera, lag in tester I rutinerna		
R45	IK 292	Se 215		
R46	IK 299	Se R30		
R47	IK 300	Se 215		
R48	IK 307	Se R39, kravställ leverantör med rätt insyn I dennes processer		
R49	IK 308	Se R44, samt se över processerna för testning		
R50	IK 328	Se R32		
R51	IK329	Se till att korrekta kontaktlistor finns upprättade		
R52	IK 331	I förvaltningsplan och avtal, säkerställ process för incidenthantering		
R53	IK 335	I dialog med SÄ, säkerställ på vilket sätt systemet ska utvecklas, följa utvecklingen, I förvaltningsplan definiera process för återkoppling		

Rnr	ID nr	Åtgärd	Ansvarig	Status
R54	IK 337	I förvaltningsplan, fastställ rutin för incidenthantering		
R55	IK 342	Se R54 samt se over loggning		
R56	IK 343	Vid uppföljning, inför rutin och process för rätt bemaning		