Miljö- och hälsoskyddsnämnden

Nämndens budget/verksamhetsplan 2022

mnkr	Nämndens ursprungliga budget 2022	Av nämnden redovisade omslutnings-förändringar	Av nämnden begärda budget-justeringar	Nämndens budget efter omslutnings-förändringar och begärda budgetjusteringar (1+2+3)	Utfall 2020 (VB 2020)	Prognos 2021 (Tertialrapport 2)
	1	2	3	4	5	6
Driftverksamhet						
Kostnader	**235,3**	**44,7**	**5,0**	**285,0**	**271,0**	**285,0**
Tillsyn/myndighetsutövning	115,8	21,0	0,0	136,8	135,2	138,4
Miljöövervakning	43,4	5,3	5,0	53,7	52,6	54,1
Miljöbilar	5,2	5,9	0,0	11,1	10,1	10,9
Energi och klimat	11,6	0,1	0,0	11,7	11,9	11,9
Gemensam verksamhet	58,7	0,2	0,0	58,9	50,2	56,7
Externfinansierade projekt	0,6	12,2	0,0	12,8	11,0	13,0
Intäkter (-)	**-96,1**	**-44,7**	**0,0**	**-140,8**	**-130,2**	**-149,9**
Tillsynsavgifter	-86,7	-21,0	0,0	-107,7	-100,1	-116,5
Miljöövervakning	-9,4	-5,3	0,0	-14,7	-13,9	-14,7
Miljöbilar	0,0	-5,9	0,0	-5,9	-4,9	-4,9
Energi och klimat	0,0	-0,1	0,0	-0,1	-0,1	-0,1
Gemensam verksamhet	0,0	-0,2	0,0	-0,2	-0,2	-0,7
Externfinansierade projekt	0,0	-12,2	0,0	-12,2	-11,0	-13,0
Verksamhetens nettokostnader exkl kap kostnad	**139,2**	**0,0**	**5,0**	**144,2**	**140,8**	**135,1**
avskrivningar	1,1	0,0	0,0	1,1	1,6	1,4
internräntor	0,0	0,0	0,0	0,0	0,0	0,0
Summa kostnader	**236,4**	**44,7**	**5,0**	**286,1**	**272,6**	**286,4**
Summa intäkter	**-96,1**	**-44,7**	**0,0**	**-140,8**	**-130,2**	**-149,9**
Netto	**140,3**	**0,0**	**5,0**	**145,3**	**142,4**	**136,5**

Miljö- och hälsoskyddsnämnden

Investeringsbudget 2022 och kommande år

Prognos (mnkr)	*Prognos 2021*	*VP 2022*	*Plan 20223*	*Plan 2024*	*Plan 2025*	*Plan 2026*
Inventarier och maskiner	1,5	1,3	1,3	1,3	1,3	1,3

Miljö- och hälsoskyddsnämnden

Verksamhetsplan 2022

Nämnderna ska redovisa samtliga pågående och planerade innovationssatsningar
Redovisningen ska innehålla en kortfattad beskrivning av satsningen samt koppling till stadens styrdokument, till exempel vision, budget eller program.
Tidplanen ska vara så exakt så möjligt och ange när projektet startade samt planerat avslut.
Under finansiering ska det anges hur projektet finansieras (externa medel, inom ram etc.). Finns samarbetsparners ska dessa anges.

Innovationssatsningar

Namn på satsningen	Typ av innovation (verksamhets-utveckling alternativt testbäddverksamhet)	Kortfattad beskrivning i punktform där syfte och mål framgår.	Tidplan	Finansieringen (intern och/eller extern)	Storlek på budget (inräknat arbetstid och medel för drift)	Samarbetspartners (Interna och Externa)	Ansvarig chef och ledare	Kontaktperson
Digital köldmediedeklaration	Testbäddsverksamhet	Skapa en obruten digital kedja från entreprenör till verksamhetssystem av lagstadgad deklaration av köldmedieinnehav.	2021-2022	intern	1 Mkr	Valcon	Monika Gerdhem	Åsa Hoffmann
Digitalt stöd för inspektioner	Testbäddsverksamhet	Digitalt stöd för genomförande av livsmedelsinspektioner.	2021-2022	intern	1 Mkr	SISAB, Valcon, SDF, Bravida	Daniel Persson	Kristine Fornander
Säkrare meddelanden	Verksamhets-utveckling	Utveckla ett arbetssätt med säker och systemintegrerad digital kommunikation.	2021-2022	intern	-	SLK	Mikael Nyberg	Jonas Arnqvist
Portföljstyrning, innovationsstruktur, kompetensförsörjning med Valcon	Verksamhets-utveckling	Etablera ett gemensamt arbetssätt för att identifiera och prioritera behov och krav	2021-2022	intern	3 Mkr	Valcon	Anna Hadenius	Malin Täppefur
App Luft Stockholm luft	Testbäddsverksamhet	Vidareutveckling med målsättning att ge medborgarna information om [illegible]	2022	intern	100 tkr	Tieto	Malin Täppefur	Magnuz Engardt
Geofencingutrustning i minst två av stadens bilar	Testbäddsverksamhet	Testa geofencing i minst två av stadens bilar. Om det fungerar väl införa geofencing i alla nya bilar.	2021 -	internt	-	Fordonsansvariga hos de förvaltningar och bolag som har fordon	Eva Sunnerstedt	Elisabeth John

Stockholms stad

Nämnd/bolag: Miljö- och hälsoskyddsnämnden

Redovisning av grundläggande baskrav för informationssäkerhet

Vid frågor kontakta Funktionen för stadsövergripande informationssäkerhet, vid avdelningen för it och digitalisering, stadsledningskontoret.
Redovisningen ska fyllas i och biläggas nämndens/bolagets verksamhetsplan för 2022.
E:post: funktion.slk.informationssakerhetcentralt@stockholm.se

Kommentar

Anvisningar

Detta dokument ger anvisningar om hur nämnder och bolag ska redovisa sin följsamhet till ett urval av kraven från stadens riktlinjer för informationssäkerhet. Urvalet är gjort för att representera några av de mest grundläggande baskraven som en nämnd/bolag har att genomföra för att kunna visa att nämnden/bolaget leder och styr risker inom informationssäkerhetsområdet enligt lagkrav och riktlinjer. Notera att det finns lagkrav på informationssäkerhetsområdet som innebär att nämnd/styrelse genom dokumentation ska kunna visa sin efterlevnad till de krav som gäller för verksamheten, varför redovisningen fyller en funktion även i det avseendet. Baskraven i denna anvisning är inte uttömmande för det informationssäkerhetsarbete som nämnden/bolaget har att genomföra enligt krav i lagar och riktlinjer.

Anvisningen är avsedd att besvaras med stöd av den *lokala informationssäkerhetssamordnaren* som är sakkunnig och utgör förvaltningschefens/bolagschefens primära stöd.

Syftet med informationssäkerhetsarbetet är att skapa förutsättningar att ändamålsenligt och effektivt nå stadens mål om trygg, effektiv och modern storstad för stadens invånare, företagare och besökare. Stockholm har som ambition att bli världsledande inom digitaliseringsområdet vilket ytterligare adresserar vikten av dessa frågor.

Den uppföljning som anvisas i detta dokument är även en del av den interna kontrollen som stadens verksamheter inklusive den centrala informationssäkerhetsfunktionen är skyldig att utöva för att visa att stadens verksamheter bedrivs i enlighet med de mål och riktlinjer som fullmäktige har beslutat.

Uppföljning av allvarliga incidenter samt förvaltningens-/bolagets utbildningsläge för sina medarbetare, i enlighet med tidigare års (2021) VP-anvisning ska fortsatt förvaltningschef/bolagschef fortsatt informera sig om varje år, som en stående punkt i ledningens genomgång.

Informationsägarens ansvar

Nämnden/bolagsstyrelsen är ytterst informationsägare, tillika personuppgiftsansvarig, i sin verksamhet. Informationsägaren ansvarar för att den information som verksamheten hanterar är riktig och tillförlitlig samt ansvarar för hur informationen hanteras och sprids. Det är därför ett budgetuppdrag för nämnder och bolag att arbeta systematiskt och ändamålsenligt med informationssäkerhet.

Förvaltnings- och bolagschef är nämnden/styrelsens operativa informationsägarrepresentant i linjen. Förvaltnings- och bolagschef ansvarar för styrningen och resurssättningen av det lokala informationssäkerhetsarbetet. Förvaltningschef/bolagschef ska årligen tillse att verksamhetsplanen omfattar relevanta informationssäkerhetsaktiviteter samt följa upp utfallet av detta arbete. Avsikten med denna anvisning är att hjälpa förvaltnings- och

Redovisning av grundläggande baskrav

	Krav	Status	Kommentar
1	Förvaltningschef/bolagschef har inrättat en *ändamålsenlig organisation* [1] med tillräckliga resurser för att hantera verksamhetens aktiviteter[2] för informationssäkerhet inklusive dataskydd samt övriga områden[3].	Ja	
2	Förvaltningschef/bolagetschef har tillsett att dataskyddsombudet har en *självständig och oberoende ställning* [4] och rapporterar till nämnd/styrelse[5].	Ja	
3	Förvaltningschef/bolagschef har tillsett a) att verksamhetens informationsmängder[6] har kartlagts samt b) att de viktigaste informationsmängderna även har klassat och riskbedömts.	a) Ja b) Ja	a) b)
4	Förvaltningschef/bolagschef har tillsett att verksamheten, utifrån riskprioritering[7], har följt upp implementeringen av skyddsåtgärder för de viktigaste informationsmängderna. Skyddsåtgärderna berör både den egna verksamheten samt leverantörer/biträden.	Nej	Förvaltningen har en helt digital ärendehantering sedan 2011. Fokus har därför legat på att informationsklassificera de olika system som verksamheten hanterar data i. Det innebär dock att ingen övergripande sammanvägning av informationsklassningar och riskprioritering har gjorts. Detta ingår i handlingsplan för 2022.
5	Förvaltningschef/bolagschef har säkerställt att registerförteckningen ger en rättvisande bild av verksamhetens personuppgiftsbehandlingar och hålls uppdaterad.	Ja	
6	Förvaltningschef/bolagschef har informerat sig om att verksamhetens informationssäkerhetsrisker hanteras i en handlingsplan[8], samt beslutat om vilka av dessa som tas om hand i verksamhetsplanen för nästkommande år.	Ja	

Fotnoter:

1) Olika verksamheter behöver utforma och införa stöd på olika sätt för att få bästa effekt, det är det som avses med begreppet *ändamålsenlig organisation.*

2) *Exempel på möjliga aktiviteter som ska utföras för att informationssäkerhetsarbetet inkl. dataskydd följer nedan. Aktiviterna utgör en sorts verktygslåda:*
Informationsklassning, riskanalys, riskbehandling, behörighetsstyrning, uppföljning av behörigheter, kravställning i avtal, säkerhetshantering i förvaltningsarbete, upphandlingar, och projekt, uppföljning av skyddsåtgärder för egen- resp. leverantörs verksamhetprojekt för etablering av dataskydd, registerförteckningar, konsekvensbedömningar, upprättande av personuppgiftsavtal med instruktioner, översyn och statusrapportering, inventering och hantering av 3:e-landsöverförande, juridisk omvärldsbevakning avs. GDPR och dataskyddspraxis

3) Övriga områden som ställer säkerhetskrav varierar beroende på den verksamhet som bedrivs och kan t.ex. avse NIS-direktivet, patientdatalagen, tillgänglighetsdirektivet, m.m.

4) Dataskyddsombudet (DSO) ska kunna arbeta självständigt och oberoende, utan att bli påverkad av andra inom organisationen. Det är därför viktigt att dataskyddsombudet inte har andra arbetsuppgifter som kan krocka med rollen som dataskyddsombud. (källa IMY, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/dataskyddsombud/)

Om dataskyddsombudet företräder arbetsgivaren i en *chefsroll* eller har andra utföraruppdrag i linjen såsom *arkivarie* eller deltar operativt i säkerhetsarbetet i rollen som *lokal informationssäkerhetssamordnare* så utgör det ett hinder för ombudets självständighet och oberoende. Den personuppgiftsansvarige (PuA) råder över ändamål och medel vilket dataskyddsombudet måste vara frikopplad från.

5) Dataskyddsombudet ska rapportera direkt till den personuppgiftansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå. (källa: GDPR Artikel 38.3)

6) Det är verksamhetens information som ska skyddas, därför behöver verksamhetens information först kartläggas. Med informationsmängd avses en logisk sammanhängade gruppering av information exempelvis inom en process. Olika verksamheter hanterar olika information beroende på verksamhetens uppdrag och de aktiviteter som följer av uppdraget, t.ex. för en stadsdelsnämnd, en fackförvaltning eller ett av stadens bolag.

7) Efter en genomförd klassning får verksamheten ut en lista över de skyddsåtgärder som verksamheten behöver arbeta med för att skydda informationen. Riskprioritering syftar till att skilja på höga och låga risker i förvaltningarnas/bolagens verksamheter, så att resurser kan styras till skyddsåtgärder som är mest kritiska för verksamheten. Riskprioritering utgör således ett stöd för vilka skyddsåtgärder som verksamheten väljer att tillämpa och i vilken ordning.

Priorierade risker kan exempelvis röra sårbarhet för ransomware, personuppgiftsbehandlingar med höga risker, 3:e-landsöverföringar av personuppgifter, NIS-tillgänglighetsrisker, brister i behörighetsstyrning, brister i verksamhetens rutiner, brister i verksamhetens/leverantörers uppföljning av skyddsåtgärder, ej genomförda konsekvensbedömningar för dataskydd, brister i verksamhetens mejlhantering av känslig information eller personuppgifter, framtagande av rutiner för att hantera brister, brister av skydd för känsliga personuppgifter, avsaknad eller fel i lagliga grunder för personuppgifter eller känsliga personuppgifter, avsaknad av eller brister i rutin för registerutdrag av personuppgifter, m.m.

8) För att visa på att ett ändamålsenligt och effektivt informationssäkerhetsarbete bedrivs i verksamheten över tid behöver förvaltningschef/bolagschef informera sig om att risker löpande identifieras, prioriteras och att prioriterade risker åtgärdas. Informationssäkerhetssamordnaren har den verksamhetsövergripande stödfunktionen att sammanställa sådan information från verksamheten, att informera förvaltningschef/bolagschef om prioriterade informationssäkerhetsrisker för verksamheten samt följa upp det fortsatta arbetet. Med handlingsplan avses sådan dokumentation som verksamheten använder för motsvarande planering och uppföljning av risker. En handlingsplan kan visa vilka frågor som beslutats för åtgärd, vem som anvarar för genomförandet, beräknade datum när åtgärder är genomförda samt hur uppföljning/utvärdering av åtgärder planeras och av vem. Handlingsplanen bör omfatta risker från för verksamheten relevanta kravområden såsom riktlinjer för informationssäkerhet, dataskydd, NIS-direktivet, patientdatalagen, tillgänglighetsdirektivet m.fl.