

# Stadsdelsnämnd Östermalm

Dnr: ÖST 2021/939 Bilaga 1

## Investeringsbudget 2022

Utgifter mnkr	Prognos t o m 2021	Budget 2022	Plan 2023	Plan 2024	Plan 2025	Plan 2026	Totalt projektet		
	(1)	(2)	(3)	(4)	(5)	(6)	(7) Genomf. beslut	(8) Avvikel. mot gfb	(9) Prognos
<b>Investeringsprojekt</b>									
Stadsmiljöprojekt									
Parkinversteringar	3,0	1,5	4,0	1,1			1,5		0,0
Ruddamsparken		3,0	1,0	5,0			8,1		
Tessinparkens parklek							6,0		
Motalaparkens plaskdam									
<b>Reinversteringar</b>									
Humlegården		0,5	1,0	1,5			3,0		
Ruddamsparken		0,5					0,5		
Innergårdar i Hjorthagen		0,5					0,5		
Kaknäs lekplats		0,5	2,0				2,5		
Tessinparkens parklek		2,0					2,0		
<b>Nycklade investeringsmedel</b>		10,2							0,0
Nycklade investeringsmedel									0,0
<b>Summa investeringsprojekt</b>	<b>0,0</b>	<b>18,7</b>	<b>8,0</b>	<b>7,6</b>	<b>0,0</b>	<b>0,0</b>	<b>24,1</b>	<b>0,0</b>	<b>0,0</b>
<b>Maskiner och inventarier</b>		2,2							
<b>UTGIFTER TOTALT</b>	<b>0,0</b>	<b>20,9</b>	<b>8,0</b>	<b>7,6</b>	<b>0,0</b>	<b>0,0</b>	<b>24,1</b>	<b>0,0</b>	<b>0,0</b>

- Nämndens prognos för projektens investeringsutgifter t.o.m. 2021
- Nämndens verksamhetsplan, inom av KF beslutad planeringsnivå i budget 2022, se bilaga 3.
- Nämndens inriktning för 2023-2026, inom av KF beslutade planeringsnivåer i budget 2022.
- Totalt beslutad utgift under projektets genomförandeperiod enligt genomförandebeslut. I det fall endast inriktningsbeslut föreligger anges investeringsutgiften enligt inriktningsbeslutet.
- Avvikelse jämfört med totalt beslutad investeringsutgift (kolumn 7). (+) ökade utgifter, (-) minskade utgifter.
- Prognos = totalt beslutad utgift + avvikelse

## Stadsdelsnämnd Östermalm

### Resultatenheter 2022

Respektive nämnd ska besluta om vilka enheter som är resultatenheter med en beslutsats. Ange nedan vilka enheter som är resultatenheter och vilka som eventuellt avslutades under 2021. Fördela resultatenheterna per verksamhetsområde.

Resultatenhetens namn
Centrala Östermalms förskolor
Engelbrekt-/Gårdets förskolor
Hedvig Eleonora förskolor
Norra Djurgårdstadens förskolor
Dagverksamheterna Östermalm





Stimulansbidrag för utbyggnad av boenden för äldre och personer med fysisk och psykisk funktionsnedsättning - underlag för ansökan  
Verksamhetsplan 2022

<b>Ansökande nämnd:</b>	
Kontaktperson: (namn, tel)	
<b>Objekt: (adress, fastighet, fastighetsägare/hyresvärd etc)</b>	
Bedömt av referens-/genomförandegrupp: (åååå-mm-dd)	
Skede:	
Lagrum:	
Verksamhetsområde:	
Boendeform:	
Upplåtelseform:	
Inflyttningsklart: (månad åååå)	
<b>Antal lägenheter:</b>	
Kort beskrivning av lägenhetstyper och storlekar:	
Total area: (kvm)	
varav lgh-area: (kvm)	
Total hyra: (kr/år)	
varav lgh-hyra: (kr/år)	
Hyresmätkt: (kr/år)	
Hyresrid: (tillsvidare, antal månader/år)	
<b>Sökt belopp (mmlkr)</b>	
Beställarsöd:	
Förprojektering/projektering:	
Särproduktion:	
Särkostnader:	
<b>Totalt: (ska stämma med beslutsmening)</b>	<b>0</b>
Kommentarer:	



## 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.informationssakerhet@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 förvaltnings-/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 resursutövningen av det lokala informationssäkerhetsarbetet.

Förvaltningschef/bolagschef ska själva tillse att verksamhetsbolagen omfattar relevanta informationssäkerhetsaktiviteter samt följa upp utförligt avsedda arbete. Avsikten med denna anvisning är att biläggas förvaltnings- och

## Redovisning av grundläggande baskrav

Krav	Status	Kommentar
Förvaltningschef/bolagschef har inrättat en <i>ändamålsenlig organisation</i> <sup>1</sup> med tillräckliga resurser för att hantera verksamhetens aktiviteter <sup>2</sup> för informationssäkerhet inklusive dataskydd samt övriga områden <sup>3</sup> .	Ja	Informationssäkerhetsansvining med tydliggörande av roller och ansvar behövs upprättas. Ett informationssäkerhetsnätverk bör upprättas med representanter från avdelningarna för förbättrad implementering av informationssäkerhetsarbetet i verksamheterna.
Förvaltningschef/bolagschef har tillsett att dataskyddsbududet har en <i>självständig och oberoende ställning</i> <sup>4</sup> och rapporterar till nämnd/styrelse <sup>5</sup> .	Ja	

3	Förvaltningschef/bolagschef har tillsett a) att verksamhetens informationsmängder <sup>6</sup> har kartlagts samt b) att de viktigaste informationsmängderna även har klassat och riskbedömts.	a) Ja b) Nej	b) Delvis genomfört. Klasseringsarbetet pågår med prioritering av informationsmängder som berörs av NIS-direktivet. Arbetet med informationsklassningar kommer att intensifieras under 2022
4	Förvaltningschef/bolagschef har tillsett att verksamheten, utifrån riskprioritering <sup>7</sup> , har följt upp implementeringen av skyddsåtgärder för de viktigaste informationsmängderna. Skyddsåtgärderna berör både den egna verksamheten samt leverantörer/biträden.	Nej	Delvis genomfört. Skyddsåtgärder framtagna i de klassningar som genomförts. Riskbedömningar följs upp löpande utifrån tex incidenter, riskobservationer, uppföljning av registerbehandlingar, konsekvensbedömningar m.m.
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 <sup>8</sup> , samt beslutat om vilka av dessa som tas om hand i verksamhetsplanen för nästkommande år.	Ja	Informationssäkerhetsrisker identifieras i bl a i väsentlighets- och riskanalysen och löpande i informationssäkerhetsarbetet. Handlingsplan för 2022 är under utarbetande.

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. Aktiviteterna 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 verksamhetsprojekt 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 utövaruppdrag 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 personuppgiftsansvariges 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 sammanhängande 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.

Prioriterade 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/leverantörens 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, avsaknad av eller brister i rutin för registerutdragen av personuppgifter m.m.



8) För att visa på 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. Informationssäkerhetsmyndigheten 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 ansvarar 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 informations säkerhet, dataskydd, NIS-direktivet, tillgänglighetsdirektivet m.fl.