Region Stockholm

LOKAL RIKTLINJE

Diarienummer
FSN 2026–0418

Fastighets- och servicenämndens lokala ledningssystem för informationssäkerhet och dataskydd

Gäller för serviceförvaltningen

Dokumenttyp	Fastställd	Giltig till och med
Lokal riktlinje	2026-06-17	Tills vidare
	Fastställd av	Upprättad av
	Fastighets- och servicenämnden	Ledningsstab

Innehållsförteckning

1. Inledning 3
1.1 Syfte 3
2. Ansvar och roller 4
3. Säkerhetsmål 5
4. Riskbedömning och riskhantering 5
5. Dataskydd 6
6. Uppföljning – ledningens genomgång 7

1. Inledning

Fastighets- och servicenämndens ledningssystem för informationssäkerhet och dataskydd för serviceförvaltningen baseras på Region Stockholms Riktlinje för informationssäkerhet samt dataskydd (RS 2025-0418), tillhörande regionala vägledningar och anvisningar liksom övriga tillämpliga lagar, allmänna råd, föreskrifter och styrande dokument. Det systematiska och riskbaserade arbetet bedrivs också enligt etablerade standarder med utgångspunkt i ISO/IEC 27001.

Fastighets- och servicenämndens verksamhet är beroende av en säker, tillgänglig och lagenlig informationshantering för att kunna leverera service till Region Stockholms nämnder och bolag. Verksamheten påverkas av krav enligt lagstiftning, regionala styrdokument, förändrade hotbilder, digitalisering, leverantörsberoenden samt krav på kontinuitet och beredskap.

Informationssäkerhets- och dataskyddsarbetet ska beakta verksamhetens skyddsvärda information, samhällsviktiga beroenden, offentlighetsprincipen samt behovet av att upprätthålla förtroendet för Region Stockholms verksamhet.

Enligt reglemente för regionstyrelsen och övriga nämnder (RS 2025-0345) ansvarar fastighets- och servicenämnden inom sitt verksamhetsområde för att följa lagar och andra författningar samt är personuppgiftsansvarig för den behandling av personuppgifter som sker inom nämndens serviceverksamhet. Ledningssystemet ska säkerställa ett systematiskt och riskbaserat arbete med informationssäkerhet och dataskydd och vara en integrerad del av fastighets- och servicenämndens ordinarie styrning, ledning, verksamhetsplanering, uppföljning och intern kontroll. Arbetet ska bedrivas genom att planera, genomföra, följa upp och förbättra verksamheten.

1.1 Syfte

Syftet med ledningssystemet är att säkra ett systematiskt arbete och en riskavvägd skyddsnivå i verksamheten. Ledningssystemet ska utgöra en integrerad del av fastighets- och servicenämndens ordinarie styrning, ledning, verksamhetsplanering, uppföljning och interna kontroll. Det lokala ledningssystemet avser informationshantering i såväl fysisk som digital form och syftar till att säkerställa bedömning och hantering av risker med utgångspunkt i Riktlinje för informationssäkerhet och dataskydd (RS 2025–0418).

2. Ansvar och roller

Ansvaret för informationssäkerhet samt dataskydd är kopplat till verksamhetsansvaret i alla led. Medarbetare och chefer ska ha tillräcklig kunskap och medvetenhet inom informationssäkerhet och dataskydd utifrån sitt ansvar, sina arbetsuppgifter och verksamhetens skyddsbehov. Varje nämnd och bolag ansvarar inom sitt verksamhetsområde för att informationssäkerhet och dataskydd upprätthålls. En chef är ansvarig för informationssäkerheten samt det operativa dataskyddet inom sitt ansvarsområde. I ansvaret ingår att:

- identifiera risker inom sitt verksamhetsområde,
- säkerställa att information hanteras enligt styrande dokument,
- genomföra beslutade säkerhetsåtgärder,
- följa upp brister och incidenter,
- säkerställa att informationssäkerhet och dataskydd integreras i verksamhetsutveckling och förändringsarbete.

Förvaltningschefen ansvarar inför fastighets- och servicenämnden för att ledningssystemet upprätthålls, efterlevs och utvecklas samt att det integreras i serviceförvaltningens verksamhetsstyrning, interna kontroll och verksamhetsutveckling. Förvaltningschefen ansvarar även för att styrande dokument inom informationssäkerhet och dataskydd hålls aktuella samt regelbundet följs upp och vid behov revideras. I detta arbete ska förvaltningschefen stödjas av informationssäkerhetssamordnaren och dataskyddssamordnaren.

Det operativa arbetet med samordning, genomförande, uppföljning och utveckling av informationssäkerhets- och dataskyddsarbetet ska utföras av utsedda roller och funktioner inom serviceförvaltningen. Informationssäkerhetssamordnaren och dataskyddssamordnaren har ett särskilt ansvar för att samordna, följa upp och utveckla arbetet inom sina respektive områden.

Informationssäkerhetssamordnaren och dataskyddssamordnaren ska inom ramen för sina ansvarsområden stödja verksamheten genom att identifiera behov, risker och utvecklingsområden samt verka för att krav, styrande dokument och tillämpliga regelverk efterlevs. De ska vidare följa upp och utvärdera verksamhetens arbete, initiera och stödja förbättringsåtgärder samt bidra till att verksamhetens förmåga att skydda information och hantera risker stärks. I uppdraget ingår även att ge stöd och vägledning till chefer och medarbetare, främja samverkan inom verksamheten samt verka för att informationssäkerhets- och dataskyddsarbetet är förankrat i ledningens styrning och uppföljning av verksamheten.

Följande roller, men inte uteslutande dessa, ska stödja det systematiska arbetet:

- systemförvaltare,
- informationsägare,
- ägare av it-system/objektägare,
- verksamhetsansvariga,

samt andra roller med ansvar inom informationshantering, säkerhet och digitalisering.

3. Säkerhetsmål

Informationssäkerhet och dataskydd ska stödja fastighets- och servicenämndens uppdrag genom att säkerställa en säker, lagenlig och tillförlitlig hantering av information, personuppgifter och verksamhetskritiska tjänster i enlighet med Region Stockholms krav samt beställande nämnders och bolags behov. Arbetet ska stärka konfidentialitet, riktighet, tillgänglighet och spårbarhet samt bidra till kontinuitet, motståndskraft och bibehållet förtroende även vid störningar, kriser, höjd beredskap och förändrade hotbilder.

Informationssäkerhet och dataskydd ska utformas utifrån principen om rätt säkerhet, där skyddsåtgärder, arbetssätt och kontrollnivåer anpassas utifrån verksamhetens skyddsbehov, accepterade risknivåer, lagkrav och beställande verksamheters behov. Säkerhetsåtgärder ska vara riskbaserade, proportionerliga och stödja verksamhetens förmåga att leverera en effektiv och tillförlitlig serviceverksamhet.

4. Riskbedömning och riskhantering

Riskhantering ska bedrivas som en kontinuerlig process. Informationstillgångar ska identifieras och klassificeras utifrån krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Skyddsåtgärder ska anpassas utifrån fastställda skyddsbehov och genomförda riskbedömningar. Riskbedömningar ska regelbundet ses över och revideras vid förändrade förutsättningar, såsom förändringar i verksamheten, hotbilden, informationshanteringen eller tillämpliga lagkrav. Risker ska bedömas utifrån sannolikhet och konsekvens samt hanteras genom kontrollaktiviteter och åtgärder.

Uppföljning ska ske minst en gång per år och riskägare med ansvar och befogenhet att hantera en risk ska utses. Verksamheten ska därför arbeta systematiskt med risker i tre steg: precisera vad som ska bedömas, gör riskbedömning och välj väg samt åtgärda. Processen ska säkerställa att

bedömningarna genererar konsistenta, korrekta och jämförbara resultat. Riskerna ska analyseras genom att bedöma de potentiella konsekvenser som skulle uppstå om riskerna realiseras och den realistiska sannolikheten för förekomsten av riskerna. Risknivåer ska fastställas. Identifieringen av risker inom säkerhetsområdet ska baseras på analys av sårbarheter och bedömning av faror och hot. Vid bedömning ska även hot som inte primärt riktas mot den egna verksamheten, så kallad överförd hotbild, bedömas om de skulle kunna orsaka oacceptabla störningar.
Informationssäkerhetsrisker ska identifieras med avseende på förlust av konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Riskbedömning och riskhantering ska genomföras i enlighet med vad som anges i Region Stockholms Riktlinje som reglerar arbetet med intern kontroll. Riskbedömningen ska utgå från de fastställda nivåerna för Region Stockholm:

Risknivå	**Sannolikhetsnivå**	**Konsekvensnivå**
• Mycket hög (MH) • Hög (H) • Medel (M) • Låg (L) • Mycket låg (ML)	• Mycket hög (5) • Hög (4) • Medel (3) • Låg (2) • Mycket låg (1)	• Katastrofal skada (5) • Kritisk skada (4) • Signifikant skada (3) • Mindre skada (2) • Begränsad skada (1)

5. Dataskydd

Fastighets- och servicenämnden ska inom sitt verksamhetsområde säkerställa ett systematiskt dataskyddsarbete i enlighet med dataskyddsförordningen (EU) 2016/679, Region Stockholms Riktlinje för informationssäkerhet samt dataskydd (RS 2025–0418), samt Integritetsskyddsmyndighetens (IMY) föreskrifter och allmänna råd eller andra berörda lagar och regler.
Serviceförvaltningen ska inom ramen för nämndens verksamhet:

- upprätthålla registerförteckningar,
- säkerställa rättslig grund för behandling,
- genomföra konsekvensbedömningar avseende dataskydd,
- hantera personuppgiftsincidenter,
- säkerställa registrerades rättigheter,
- säkerställa att instruktioner och personuppgiftsbiträdesavtal upprättas där så krävs

Behandling av personuppgifter ska dokumenteras i enlighet med Region Stockholms gemensamma processer och systemstöd.

Informationssäkerhetsincidenter och personuppgiftsincidenter ska rapporteras, hanteras, dokumenteras och följas upp enligt fastställda processer. Identifierade brister och avvikelser ska ligga till grund för förbättringsåtgärder.

Dataskyddsombudet ska självständigt och oberoende granska efterlevnaden av dataskyddslagstiftningen enligt artikel 37–39 i dataskyddsförordningen.

6. Uppföljning – ledningens genomgång

Nämnden ska regelbundet genomföra revision av sin informationssäkerhet och dataskydd samt göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras. Mätetal och uppföljningsmetoder ska anpassas utifrån verksamhetens behov, riskbild och skyddsvärde. Uppföljningen sker årligen genom ”ledningens genomgång” som syftar till att säkerställa det lokala ledningssystemets fortsatta lämplighet, effektivitet och ändamålsenlighet.

Uppföljning ska dokumenteras och ligga till grund för prioriteringar, förbättringsåtgärder och fortsatt utveckling av det lokala ledningssystemet. Förbättringsarbetet ska bedrivas inom ramen för Region Stockholms ledningsprocess – planera, genomföra, följa upp och agera.