



Informationssäkerhets- policy

Sibbo kommun

Innehåll

1 Centrala begrepp i informationssäkerhetspolicyn	3
2 Informationssäkerhetspolicyns betydelse	4
3 Roller och ansvar i informationssäkerhet	5
4 Principer för informationssäkerhet.....	6
4.1 Inbyggt dataskydd och dataskydd som standard.....	8
4.2 Leverantörskontroll	8
4.3 Kontinuitetshantering.....	8
4.4 Överträdelser av informationssäkerhet eller dataskydd.....	9
5 Riskbaserat förhållningssätt och hantering av datasäkerhetsrisker	9
6 Utbildning och ökad medvetenhet	9
6.1 Informering om informationssäkerhet	10
7 Dokumentets uppgifter och versionshistorik	10

1 Centrala begrepp i informationssäkerhetspolicyn

Datasäkerhet	Datasäkerhet avser skyddet av data och informationsmaterial. Datasäkerhet innebär konkreta säkerhetsåtgärder som kommunen vidtar för att skydda data och datautrustning. Datasäkerhet är starkt förknippad med förverkligande av principerna för dataskyddet.
Informationssäkerhet	Informationssäkerhet är ett omfattande begrepp som avser allt skydd av data och den information som data representerar. Med hjälp av informationssäkerhet försäkras man uppgifternas konfidentialitet, integritet och användbarhet. Bland annat skyddet av informationsmaterial, utrustningar, programvaror, datakommunikation, lokaler och verksamhet ingår i informationssäkerheten.
Dataskydd	Dataskydd avser en grundläggande rättighet som tryggar var och ens rättigheter och friheter i behandling av personuppgifter. Dataskyddet fastställer principer för när, under vilka förutsättningar och hur personuppgifter kan behandlas.
Konfidentialitet	Konfidentialitet avser att uppgifterna är tillgängliga endast för de som är berättigade att behandla dem. Uppgifterna skyddas på ett pålitligt sätt, och rätten att behandla uppgifterna grundar sig på arbetsuppgifterna och principen om lägsta behörighet. Uppgifternas och datasystemens användare identifieras på ett pålitligt sätt.
Integritet	Integritet avser att uppgifterna inte kan redigeras av andra personer än de som är berättigade till det. Med integritet säkerställs att uppgifterna och deras behandlingssätt är korrekta, högklassiga och obestridda. Uppgifterna skyddas mot olovlig eller oavsiktlig redigering eller radering.
Användbarhet	Användbarhet avser att uppgifterna och datasystemen kan användas endast av de som är berättigade till dem. De som är berättigade till uppgifterna och tjänster som hänför sig till dem kan använda dem i rätt tid.
Tekniska och organisatoriska åtgärder	Uppgifternas konfidentialitet, integritet och användbarhet säkerställs med tekniska och organisatoriska åtgärder. Tekniska och organisatoriska åtgärder avser till exempel personalutbildning, anvisningar och bestämmelser för personalen, sekretessavtal, lokalövervakning, kryptering av uppgifter, anonymisering och pseudonymisering av uppgifter, auditeringar, tekniska begränsningar och kontroller, kontroll- och övervakningssystem, uppförandekoder och certifikat.
Säkerhetsöverträdelse	Säkerhetsöverträdelse avser en fysisk eller teknisk överträdelse av datasystem. Typiska säkerhetsöverträdelser är till exempel dataintrång, överbelastningsattacker och skadeprogram. I en säkerhetsöverträdelse bryter eller tränger någon sig in i organisationens ICT-infrastruktur, utrustning eller information i organisationens datasystem. Informationen kan stjälas och exploateras. En säkerhetsöverträdelse riktas inte alltid mot

	personuppgifter. Målet kan också vara att överta utrustningar eller använda dem för kriminella ändamål.
Personuppgiftsincident	En personuppgiftsincident är en säkerhetsöverträdelse som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

2 Informationssäkerhetspolicyns betydelse

Informationssäkerhetspolicyn är en handling som fastställer genomförandet och hanteringen av datasäkerheten på den högsta nivån. Målet med informationssäkerhetspolicyn är att stödja uppnåendet av Sibbo kommuns strategiska mål. Sibbo kommuns informationssäkerhetspolicy fastställer ansvar, principer och praxis för behandling och skydd av personuppgifter samt ett system för övervakning av datasäkerhet och påföljder, som följs i genomförande och utveckling av datasäkerheten.

Informationssäkerheten grundar sig på lagstiftning, normstyrning och avtal. Tillämpningen av informationssäkerhetspolicyn begränsas inte av dataformatet eller av det sätt på vilket uppgifterna behandlas eller framställs. Policyn tillämpas under samtliga skeden av informationens livscykel.

Informationssäkerhetspolicyn gäller all verksamhet i Sibbo kommun. Även kommunens serviceleverantörer och intressentgrupper ska beakta informationssäkerhetspolicyn i sin verksamhet. Informationssäkerhetspolicyn ålägger Sibbo kommuns personal, ledning, förtroendevalda, tjänsteinnehavare samt alla andra personer som behandlar uppgifter hos eller för kommunen så som konsulter, underleverantörer och intressentgrupper oberoende av uppgifternas format.

Principerna i informationssäkerhetspolicyn och hur de tillämpas kan preciseras med riktlinjer och krav, praxis, anvisningar och andra dataskydds- och informationssäkerhetsdokument.

Kommunstyrelsen har godkänt informationssäkerhetspolicyn. Informationssäkerhetspolicyn granskas årligen och vid behov oftare om det sker betydande ändringar i dataskydds- och informationssäkerhetspraxisen, lagstiftningen eller myndighetsanvisningarna. Granskningens syfte är att säkerställa policyns aktualitet och effektivitet. Dataskydds- och datasäkerhetsgruppen ansvarar för granskningen av informationssäkerhetspolicyn.

3 Roller och ansvar i informationssäkerhet

Roller och ansvar i informationssäkerhet fördelas i Sibbo kommun enligt tabellen nedan:

Kommunstyrelsen	Kommunstyrelsen leder och övervakar informationssäkerheten och allokerar resurser för datasäkerhetsarbetet.
Kommundirektör	Informationssäkerheten i en kommun är i kommundirektörens besittning. Hen ska se till att informationssäkerheten kan genomföras på ett vederbörligt sätt. Kommundirektören tillsätter en dataskydds- och datasäkerhetsgrupp, som uppföljer genomförandet av dataskydd och informationssäkerhet, ger utvecklingsförslag och erbjuder stöd till sektorerna, huvudanvändarna av system, uppgifternas ägare och de personuppgiftsansvarige.
Sektorns ledning	Sektorns ledning ansvarar för att datasäkerheten förverkligas inom sektorns verksamhet. Sektorns ledning ansvarar för de system, register, informationsmaterial och datalager som sektorn äger. Ledningen säkerställer att medlemmarna i dataskydds- och datasäkerhetsgruppen har tillräckliga resurser och nödvändigt kunskande för att sköta sin uppgift.
Chefer	Cheferna ansvarar för att datasäkerheten genomförs i de underlydande funktionerna. Cheferna rapporterar till utöver sektorns ledning även dataskydds- och datasäkerhetsgruppen om dataskydds- och informationssäkerhetsärenden.
Den dataskyddsansvarige	Den dataskyddsansvarige ansvarar för uppgifterna i artikel 39 i EU:s dataskyddsförordning. Den dataskyddsansvarige hjälper i egenskap av organisationens expert den personuppgiftsansvarige att skapa god praxis för behandling av personuppgifter och dataskyddets höga nivå som eventuella speciallagar förutsätter. Med dessa uppgifter kan man bygga upp och upprätthålla de registrerades förtroende för den personuppgiftsansvarige.
Dataskydds- och datasäkerhetsgruppen	Dataskydds- och datasäkerhetsgruppen ansvarar för uppföljning och utveckling av genomförandet av datasäkerheten och dataskyddet. Gruppen ger stöd till sektorerna, systemadministratörerna, uppgifternas ägare och de personuppgiftsansvariga. Dataskydds- och datasäkerhetsgruppen ansvarar för styrning av datasäkerhetsprocesserna och för deras integrering i det övergripande säkerhetsarbetet samt för kommunikation om datasäkerhetsärenden inom ramen för de resurser och behörigheter som beviljats gruppen av kommunens ledning. Uppgiften inkluderar även anvisningar för och koordinering av hanteringen av datasäkerhetsrisker och informationssäkerhetsincidenter.
Digital förvaltning	Enheten Digital förvaltning ansvarar för genomförandet av datasäkerhet och teknisk övervakning i informationssystemmiljön med hjälp av de metoder som står till deras förfogande enligt lagen och som de har befullmäktigats till i samband med samarbetsförfarandet. Enheten ansvarar för fastställande och ordnande av den tekniska datasäkerheten.

	Enheten ansvarar också för systemet för identitetshantering och kontroll av användarrättigheter i enlighet med den nationella lagstiftningen och de EU-förordningar som tillämpas.
Tjänsteinnehavare, anställda, de förtroendevalda och övriga personer som är jämförbara med ett anställningsförhållande	Var och en ansvarar för sin del att datasäkerheten genomförs i de egna arbetsuppgifterna. Det är på var och ens ansvar att utan dröjsmål meddela sin chef eller och dataskydds- och datasäkerhetsgruppen, alternativt den part som är ansvarig för serviceproduktionen eller verksamheten, om man upptäcker någon hot, risk eller överträdelse gällande dataskydd.
Ägare av en uppgift, ett datasystem eller en tjänst	Ägaren ansvarar för att definiera och godkänna systemanvändare och deras användarrättigheter, att genomföra riskhanteringsmetoder, att garantera uppgifternas integritet och att klassificera uppgifterna (definiera vilka uppgifter är offentliga respektive sekretessbelagda samt utarbeta en arkivbildningsplan) samt att förstöra uppgifterna.

4 Principer för informationssäkerhet

Principerna för informationssäkerhet följs under samtliga skeden av livscykeln för behandling av personuppgifter och i uppgifternas samtliga former. Med uppgifternas livscykel avser man uppgifternas samtliga behandlingskedan från insamling till förstöring.

Med hjälp av principerna för informationssäkerhet försäkras man uppgifternas konfidentialitet, integritet och användbarhet och därmed också pålitligheten, kvaliteten och kontinuiteten av kommunens serviceproduktion, processer och övriga funktioner. Alla beslut angående informationssäkerhet fattas på grund av myndighetsförfattningar samt enligt principerna för god informationshantering och -behandling.

Skydd av uppgifterna är en väsentlig del av kommunens övergripande säkerhet och dagliga verksamhet. Datasäkerheten bygger på en kunnig personal som förbinder sig till att främja datasäkerheten. Skyddet av uppgifterna styrs med principerna för informationssäkerhet och främjas genom att ta principerna för informationssäkerhet med som en del av personalens introduktion och utbildning.

Förutsättningen för genomförande av principerna och säker användning av ny teknologi är att principerna för informationssäkerhet följs.

Sibbo kommuns centrala principer för informationssäkerhet presenteras i tabellen nedan:

Administrativ informationssäkerhet	Administrativ informationssäkerhet består av principer, ansvarsfördelning, praxis, anvisningar och resurser godkända av ledningen samt riskbedömning och övervakning.
Personalsäkerhet	Huvudvikten i personalsäkerheten ligger i att förebygga riskerna på förhand genom att kontrollera dataflödets säkerhet i arbetsprocesser och behandlingskedjor, arbetsuppgifternas tillräckliga differentiering, kontinuerlig tillsyn och personalens tillräckliga och aktuella kunskaper i datasäkerhet.

Fysisk datasäkerhet	Fysisk datasäkerhet omfattar alla de medel med vilka man strävar efter att säkerställa personernas, datamaterialens, utrustningens, lokalernas och egendomens säkerhet. Fysisk säkerhet säkerställs med bland annat byggnads- och lokalitetslösningar, fysisk och teknisk passerkontroll samt säkerhetspraxis för förebyggande av brand-, vatten-, el-, ventilations- och inbrottsskador.
Säkerhet i datamaterialet	Säkerhet i datamaterialet inbegriper säkerställande av datamaterialets konfidentialitet, integritet och användbarhet. Målet är att förebygga förstörelse av uppgifter eller oavsiktlig redigering samt att säkerställa klassificering, skydd, korrekt behandling, förvaring och förstörande av datamaterialet.
Säkerhet vid användning	Säkerhet vid användning inbegriper bland annat säkra principer för användning av systemen, kompetens i de system som används, övervakning av behandlingen av personuppgifterna, utrustningens driftsäkerhet och datasäkerhetsuppdateringar, lösenordspraxis, hantering av behörigheter som beviljas enligt arbetsuppgifter, säkerställande av kontinuiteten samt underhåll av de mest centrala funktionerna, processbeskrivningarna och anvisningarna.
Datorsäkerhet	Datorsäkerhet omfattar de åtgärder för informationssäkerhet som hänför sig till databehandlingsutrustningens och telekommunikationsutrustningens användbarhet och funktionalitet, fastställande av utrustningens sammansättningar samt tillgången till reservdelar och tillbehör.
Programvarubaserat skydd	Programvarubaserat skydd inbegriper förfaranden och åtgärder som riktas mot operativsystem och programvaror för att säkerställa datasäkerheten: identifikation, isolering, åtkomsthantering och verifiering av programvaror, kontroll och övervakning, loggar, kvalitetssäkring samt åtgärder för underhåll och uppdatering av programvaror.
Kommunikationssäkerhet	Uppgifters konfidentialitet, integritet och användbarhet säkerställs i informationsutbytet inom systemet eller mellan organisationerna med kommunikationssäkerhet. Det centrala målet är att säkerställa meddelandens ursprung, integritet och konfidentialitet.

4.1 Inbyggt dataskydd och dataskydd som standard

Sibbo kommun följer principerna för inbyggt dataskydd och dataskydd som standard. Behandlingen av personuppgifter följer de principer för behandling av personuppgifter som bestäms i dataskyddsförordningen och andra bestämmelser om behandling av personuppgifter.

Dessa tekniska och organisatoriska åtgärder garanterar att man som standard samlar in enbart sådana personuppgifter som är nödvändiga för behandlingsändamålet. Dataskyddsprinciperna beaktas i all verksamhet redan i det tidigaste möjliga skedet och nödvändiga tekniska och organisatoriska åtgärder vidtas i förhållande till risknivån.

Att dataskyddsprinciperna följs i insamling och behandling av personuppgifter säkerställs genom att säkerställa att bland annat

- man enbart samlar in sådana personuppgifter som är nödvändiga för det planerade behandlingsändamålet
- personuppgifter enbart behandlas för det planerade behandlingsändamålet
- uppgifter inte samlas in i större mängder eller för en längre tid än som är nödvändigt för det aktuella behandlingsändamålet
- tillgång till uppgifterna är som standard inte tillåtet för ett obegränsat antal personer
- de registrerades rättigheter försäkras
- personuppgifterna skyddas med nödvändiga datasäkerhetsåtgärder.

De krav som ställs för till exempel övervakning av behörighet och användning av datasystem ska beaktas i ett så tidigt skede som möjligt redan när man anskaffar och utvecklar olika applikationer.

Dataskyddet behandlas närmare i Sibbo kommuns dataskyddspolicy.

4.2 Leverantörskontroll

Ansvar och plikter gällande datasäkerhet och dataskydd beaktas i avtalen mellan kommunen och olika parter. Då avtal ingås säkerställs att avtalsvillkoren uppfyller de informationssäkerhetskrav som riskbedömningen förutsätter. Personer som utarbetar leverans- och entreprenadavtal ansvarar för att säkerställa att dataskyddsnivån i de köpta tjänsterna motsvarar bestämmelserna och anvisningarna samt de gällande föreskrifterna både när man ingår avtalet och under uppdraget. I avtalen ska ingå rätt att utföra auditering av leverantören, och denna rätt utnyttjas vid behov. Regelbundna planerings- och uppföljningspalavrer ordnas med leverantören, och i dem behandlas även datasäkerhetsärenden.

4.3 Kontinuitetshantering

Risker som äventyrar kontinuiteten av kommunens verksamhet identifieras och kommunen förbereder sig inför dem med planerna för kontinuitet och återhämtning och tillhörande reservarrangemang. Kontinuitetshanteringens fokuserar på förebyggande av problem och risker samt snabb återhämtning efter incidenterna. Kontinuitetshanteringens innefattar beredskap inför cyberhot och bedömning av skyddspraxisens tillräcklighet. Även avtalsparterna förutsätts att de regelbundet identifierar risker som äventyrar verksamhetens kontinuitet samt att deras planer för kontinuitet och återhämtning är ajour.

4.4 Överträdelser av informationssäkerhet eller dataskydd

Olika arrangemang kring datasäkerhet och dataskydd genomförs på så sätt att det inte krävs orimliga resurser för att utreda eventuella säkerhetsincidenter i efterhand. Överträdelser av informationssäkerhet, informationssäkerhetsincidenter och personuppgiftsincidenter hanteras enligt hanteringsprocessen. Varje anställd i organisationen är förpliktad att göra en anmälan om de upptäcker risker, avvikelser eller övriga motsvarande situationer som kan äventyra datasäkerheten. Dataskydds- och datasäkerhetsgruppen ser till att anvisningarna om registrering av personuppgiftsincidenter är ajour. Sektordirektörerna ansvarar för att incidenterna utreds utan dröjsmål och de upptäckta riskerna fås under kontroll.

Då personuppgiftsincidenter ska anmälas till tillsynsmyndigheten och meddelas till den registrerade ska det göras i enlighet med lagen och kommunens anvisningar. Sibbo kommuns dataskyddsansvarige är kontaktpersonen till tillsynsmyndigheten.

5 Riskbaserat förhållningssätt och hantering av datasäkerhetsrisker

Kommunen bedömer de risker som förknippas med behandling av personuppgifter och väljer nödvändiga förvaltnings- och datasäkerhetsåtgärder enligt den uppskattade risknivån i egenskap av den personuppgiftsansvarige. Man ska genom ett riskbaserat förhållningssätt bedöma på vilket sätt datasäkerheten genomförs. Kommunens olika system klassificeras enligt en bedömning om kritikalitet. De kritiska systemens säkerhetsarrangemang kontrolleras regelbundet och deras funktionsduglighet testas vid behov. Datasäkerheten och dess hanteringssätt utvecklas fortsatt med beaktande av bedömning och analys av datasäkerhetsrisker, praktiska erfarenheter och informationssäkerhetens allmänna utveckling.

6 Utbildning och ökad medvetenhet

Anvisningar som styr informationssäkerhetsarbetet i hela kommunen utarbetas i administrativt samarbete. Anvisningar om informationssäkerhet inkluderas i kommunens övriga anvisningar och i processernas olika skeden med beaktande av principerna i denna policy.

Sibbo kommun ska bevisa att personalens kunnande om datasäkerhet och dataskydd är ajour. Kunskaper i dataskydd och datasäkerhet bevisas med avlagda utbildningar, olika utbildningsintyg samt genom att följa med personalens kunnande. Chefernas övervakningsrätt och -ansvar innefattar övervakning av att datasäkerhetsanvisningarna följs.

Sibbo kommun förutsätter att alla anställda undertecknar en datasäkerhetsförbindelse i början av anställningsförhållandet. För att garantera personalens kunnande förutsätter kommunen därtill att samtliga anställda utför årligen utbildningar i datasäkerhet och dataskydd. Även förtroendevalda ska utföra datasäkerhets- och dataskyddsutbildningar. Därtill ordnar kommunen årligen dataskyddsutbildningar som riktas till specifika personalgrupper.

6.1 Informering om informationssäkerhet

Informationssäkerhetspolicyn fastställer de gällande principerna för informationssäkerhet. Hela personalen informeras om dokumentet. Efter det att policyn har blivit godkänd publiceras den i kommunens interna nätverk och externa webbplats och personalen informeras om den även på andra sätt. Kommunikation om informationssäkerhet sker i allmänhet via Dataskydds- och datasäkerhetsgruppen och ledningsgrupperna.

7 Dokumentets uppgifter och versionshistorik

Version	Datum	Ändringar	Gjord av
1.0	21.7.2022	Den första godkända versionen	Dataskyddsteamet/den dataskyddsansvarige
2.0	4.2.2025	Utkast 1	Digital förvaltning
2.0	24.2.2025	Utkast 2	Den dataskyddsansvarige
2.0	25.2.2025	Den andra godkända och publicerade versionen	Dataskydds- och datasäkerhetsgruppen

Dokumentets namn	Sibbo kommuns informationssäkerhetspolicy
Ägare	Dataskydd - och datasäkerhetsgruppen, Sibbo kommun
Godkänt av	Kommunstyrelsen
Datum för godkännandet	29.09.2025