Datasäkerhetspolicy

Sibbo kommun

SIPOO
SIBBO

Innehåll

1 Centrala begrepp i datasäkerhetspolicyn 3

2 Vikten av datasäkerhetspolicyn 4

3 Roller och ansvar inom datasäkerhet 4

4 Principer för datasäkerhet 5

4.1 Inbyggt dataskydd och dataskydd som standard 6

4.2 Leverantörshantering 7

4.3 Kontinuitetshantering med avseende på verksamheten 7

4.4 Överträdelser med avseende på datasäkerhet och dataskydd och deras påföljder 7

6 Utbildning och ökad medvetenhet 8

6.1 Kommunikation om datasäkerhetsfrågor 8

7 Dokumentinformation och versionshistorik 8

1 Centrala begrepp i datasäkerhetspolicyn

Datasäkerhet	Datasäkerheten säkerställer datas konfidentialitet, integritet och användbarhet. Datasäkerhet omfattar bland annat skyddande av data, datamaterial, utrustning, programvara, datakommunikation, lokaler och verksamhet. Datasäkerheten är nära förknippad med genomförandet av dataskyddsprinciperna.
Dataskydd	Dataskydd innebär en grundläggande rättighet som tryggar var och ens rättigheter och friheter vid behandling av personuppgifter. Dataskyddet fastställer principerna för när, under vilka förutsättningar och hur personuppgifter kan behandlas.
Konfidentialitet	Konfidentialitet innebär att data endast är tillgänglig för dem som har rätt att använda den. Data skyddas på ett tillförlitligt sätt och rätten att behandla data baserar sig på det behov som arbetsuppgifterna kräver och principen om minimirättigheter. Användare av data och system identifieras på ett tillförlitligt sätt.
Integritet	Integritet innebär att data inte kan ändras av någon annan än den som är berättigad till det. Riktigheten, kvaliteten och obestridligheten hos data och databehandlingsmetoderna säkerställs. Data skyddas mot obehörig eller oavsiktlig ändring eller radering.
Användbarhet	Användbarhet innebär att data och datasystemen kan användas av dem som har rätt att använda dem. Data och de tjänster som är baserade på dem är tillgängliga för befullmäktigade personer vid rätt tidpunkt.
Tekniska och organisatoriska åtgärder	Tekniska och organisatoriska åtgärder vidtas för att säkerställa datas konfidentialitet, integritet och användbarhet. Tekniska och organisatoriska åtgärder omfattar exempelvis utbildning av personal, anvisningar och föreskrifter, sekretessavtal, övervakning av lokaler, kryptering av data, anonymisering och pseudonymisering av data, auditering, tekniska begränsningar och kontroller, kontroll- och övervakningssystem, regler för praxis och införande av certifikat.
Brott mot datasäkerhet	Ett brott mot datasäkerheten är en fysisk eller teknisk kränkning som riktar sig mot ett datasäkerhetssystem. Typiska former av brott mot datasäkerheten inkluderar dataintrång, överbelastningsangrepp och skadlig programvara. Ett brott mot datasäkerheten innebär att ett intrång sker i organisationens datasystem och stulna data utnyttjas. Ett brott mot datasäkerheten riktar sig inte alltid mot personuppgifter.
Personuppgiftsincident	En personuppgiftsincident innebär ett brott mot datasäkerheten som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

2 Vikten av datasäkerhetspolicyn

Datasäkerhetspolicyn är det övergripande dokument som definierar genomförandet och hanteringen av datasäkerhet. Syftet med datasäkerhet är att stödja genomförandet av Sibbo kommuns strategiska mål. Sibbo kommuns datasäkerhetspolicy fastställer ansvaren, principerna och förfarandena för behandling och skydd av data.

Datasäkerheten grundar sig på lagstiftning, normstyrning och avtal. Tillämpningen av datasäkerhetspolicyn är inte bunden till dataformatet eller det sätt på vilket data behandlas eller presenteras. Policyn tillämpas i samtliga skeden av datas livscykel.

Datasäkerhetspolicyn gäller all verksamhet i Sibbo kommun. Även de serviceproducenter och intressentgrupper som kommunen anlitar ska beakta datasäkerhetspolicyn i sin verksamhet. Datasäkerhetspolicyn är förpliktande för Sibbo kommuns personal, ledning, förtroendevalda, tjänsteinnehavare och alla andra personer som behandlar uppgifter hos eller för kommunen så som konsulter, underleverantörer och intressentgrupper oberoende av datas format.

Principerna som följer av datasäkerhetspolicyn samt deras tillämpning kan specificeras med riktlinjer och krav, rutiner, instruktioner och annan dokumentation om datasäkerhet.

Kommunstyrelsen har godkänt datasäkerhetspolicyn. Datasäkerhetspolicyn ses över årligen och vid behov oftare om det sker betydande förändringar i datasäkerhets- eller dataskyddsrutinerna, lagstiftningen eller myndigheternas anvisningar. Syftet med översynen är att säkerställa att policyn är aktuell och effektiv. Dataskydds- och datasäkerhetsgruppen ansvarar för översynen av datasäkerhetspolicyn.

3 Roller och ansvar inom datasäkerhet

Rollerna och ansvaren inom datasäkerheten i Sibbo kommun är fördelade enligt tabellen nedan:

Kommunstyrelsen	Ansvarar för ledningen, resurstilldelningen och tillsynen av datasäkerheten.
Kommundirektören	Innehar uppgiften som ägare av datasäkerheten i kommunen och skapar förutsättningar för ett korrekt genomförande av datasäkerheten. Vid behov tillsätter kommundirektören en grupp som följer upp hur datasäkerheten och -skyddet genomförs, ger utvecklingsförslag och stödjer sektorernas dataskyddsombud och systemadministratörer.
Sektorledningen	Ansvarar för att datasäkerheten genomförs i den verksamhet som leds av den.
Cheferna	Ansvarar för att dataskyddet genomförs i den verksamhet som är underordnad dem. Cheferna rapporterar om dessa ärenden både till sektorledningen och till datasäkerhetsteamet.
Datasäkerhetsteamet	Ansvarar för styrning av datasäkerhetsprocesserna och för deras integrering i det övergripande säkerhetsarbetet samt för kommunikation om datasäkerhetsärenden inom ramen för de resurser och befogenheter som beviljats teamet av kommunens ledning. Uppgiften omfattar planering, styrning, uppföljning och utveckling av datasäkerhetsarbetet samt koordinering av

	åtgärderna vid risker och avvikelser relaterade till datasäkerheten. Chief Digital Officer rapporterar till kommundirektören. Datasäkerhetsteamet tillsammans med it-serviceproducenter som följer teamets anvisningar ansvarar för genomförandet av datasäkerhet och teknisk övervakning i it-miljön med hjälp av de metoder som står till deras förfogande enligt lagen och som de har befullmäktigats till i samband med samarbetsförfarande.
Tjänsteinnehavarna, arbetstagarna, de förtroendevalda och andra personer i en position som kan jämföras med ett anställningsförhållande	Ansvarar för egen del för genomförandet av datasäkerheten i sina egna arbetsuppgifter. Det är på var och ens ansvar att utan dröjsmål meddela sin chef eller kommunens dataskyddsombud, alternativt den part som är ansvarig för en serviceproduktion eller verksamhet, om man upptäcker något hot, risk eller överträdelse gällande dataskydd.
Ägaren av data, datasystem eller en tjänst	Ansvarar med avseende på sitt ägande för definiering och godkännande av användare och deras användarrättigheter, genomförande av riskhanteringen, säkerställande av dataintegritet och klassificering av data (definiering av offentlighet och sekretess samt arkivbildning) samt förstöring av data.

4 Principer för datasäkerhet

Principerna för datasäkerhet följs under samtliga skeden av databehandlingens livscykel och i alla former av data. Med informationens livscykel avser man informationens samtliga behandlingskeden från uppkomst till makulering.

Principerna för datasäkerhet säkerställer datas konfidentialitet, integritet och användbarhet och därmed tillförlitligheten, kvaliteten och kontinuiteten i kommunens tjänsteproduktion, processer och andra funktioner. Alla beslut angående datasäkerhet fattas på grund av myndighetsförfattningar samt enligt principerna för god informationshantering och -behandling.

Skydd av data är en väsentlig del av kommunens övergripande säkerhet och dagliga verksamhet. Datasäkerheten bygger på en kunnig personal som är engagerad i datasäkerhetsfrågorna. Datasäkerhetsprinciperna styr dataskyddet och främjas genom att inkludera datasäkerhetsprinciperna i personalens introduktion och utbildning.

Iakttagande av datasäkerhetsprinciperna är en förutsättning för implementering av dataskyddsprinciperna och säker användning av ny teknik.

I tabellen nedan presenteras de viktigaste principerna för datasäkerhet i Sibbo kommun:

Administrativ datasäkerhet	Den administrativa datasäkerheten består av de principer som godkänts av ledningen samt av ansvarsfördelning, handlingssätt, anvisningar, resurser som reserverats för ändamålet och av riskbedömning och tillsyn.
Personalsäkerhet	Huvudvikten inom personalsäkerheten ligger på att undvika risker i förväg genom att säkerställa att dataflödena i arbetsprocesserna och i behandlingskedjorna är säkra, arbetsuppgifterna är

	tillräckligt separerade, tillsynen är kontinuerlig och personalens kunnande om datasäkerhet är aktuell.
Fysisk datasäkerhet	Fysisk datasäkerhet omfattar alla metoder som syftar till att skydda säkerheten hos personer, datamaterial, utrustning, lokaler och egendom. Fysisk säkerhet säkerställs till exempel genom byggnads- och lokallösningar, fysisk och teknisk passerkontroll, säkerhetsrutiner i syfte att förebygga brand-, vatten-, el-, luftkonditionerings- och inbrottsskador.
Säkerhet för datamaterial	Säkerhet för datamaterial inkluderar säkerställande av datamaterials konfidentialitet, integritet och användbarhet. Syftet är att förhindra förstöring eller oavsiktlig ändring av data och att säkerställa klassificering, skydd, korrekt behandling, förvaring och förstöring av datamaterial.
Säkerhet vid användning	Säkerhet vid användning omfattar till exempel säkra användningsprinciper för system, kunskap om de system som används, övervakning av databehandlingshändelser, driftstillförlitlighet och datasäkerhetsuppdateringar med avseende på utrustning, lösenordspraxis, hantering av användarrättigheter baserat på arbetsuppgifter, säkerställande av kontinuitet samt upprätthållande av beskrivningar och instruktioner för de viktigaste funktionerna och processerna.
Utrustningssäkerhet	Utrustningssäkerhet innebär åtgärder med vilka datasäkerhet genomförs i fråga om databehandlings- och datakommunikationsutrustning. Dessa omfattar användbarhet, funktionalitet, specifikation av konfigurationer och tillgång till reservdelar och tillbehör.
Programvarusäkerhet	Programvarusäkerhet omfattar åtgärder med vilka datasäkerhet säkerställs i fråga om operativsystem och programvara. Dessa omfattar förfaranden för autentisering, isolering, åtkomstkontroll och backup, övervaknings- och tillsynsåtgärder, loggförfaranden, kvalitetssäkringsförfaranden samt åtgärder för programvaruunderhåll och uppdatering.
Säkerhet för datakommunikation	Säkerhet för datakommunikation säkerställer konfidentialitet, integritet och användbarhet för data som överförs inom ett system eller mellan organisationer. Ett viktigt mål är att säkerställa meddelandenas autenticitet, integritet och konfidentialitet.

4.1 Inbyggt dataskydd och dataskydd som standard

Sibbo kommun följer principerna om inbyggt dataskydd och dataskydd som standard i sin verksamhet. Vid behandling av personuppgifter ska dataskyddsförordningen och annan tillämplig reglering om behandling av personuppgifter följas.

Genom tekniska och organisatoriska åtgärder säkerställs att man som standard enbart behandlar sådana personuppgifter som är nödvändiga för behandlingsändamålet. Dataskyddsprinciperna beaktas i all verksamhet från ett så tidigt skede som möjligt och lämpliga tekniska och organisatoriska åtgärder vidtas i förhållande till risknivån.

Efterlevnad av dataskyddsprinciperna vid insamling och behandling av personuppgifter säkerställs bland annat genom att se till att

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

Dataskyddet behandlas närmare i Sibbo kommuns dataskyddspolicy.

4.2 Leverantörshantering

Ansvaret och skyldigheterna i samband med datasäkerhet och dataskydd beaktas i kommunens avtal med olika parter. När avtal ingås säkerställs att de krav på datasäkerhet som riskbedömningen kräver uppfylls i avtalsvillkoren. De personer som upprättar upphandlings- och outsourcingavtal ansvarar för att nivån på datasäkerheten hos köptjänster uppfyller föreskrifter, anvisningar och gällande bestämmelser både vid tidpunkten för ingåendet av avtalet och under hela uppdragstiden. I avtalen förbehåller sig kommunen rätten att granska leverantören, och denna rätt utövas vid behov. Med leverantören hålls regelbundna planerings- och uppföljningsmöten där även datasäkerhetsfrågor behandlas.

4.3 Kontinuitetshantering med avseende på verksamheten

I kommunens verksamhet identifieras risker som hotar kontinuiteten och beredskap för dem skapas genom kontinuitets- och återhämtningsplaner och tillhörande reservarrangemang.
Kontinuitetssäkringen är inriktad på att förebygga problem och risker samt på snabb återhämtning från avvikande situationer. Kontinuitetshanteringen omfattar beredskap för cyberhot och en bedömning av tillräckligheten av skyddsrutinerna inom cybersäkerhet. Även av avtalspartners krävs att de regelbundet identifiera risker som hotar kontinuiteten i deras verksamhet och har uppdaterade planera för kontinuitet och återhämtning.

4.4 Överträdelser med avseende på datasäkerhet och dataskydd och deras påföljder

Datasäkerhets- och skyddsarrangemang genomförs på ett sådant sätt att säkerhetsöverträdelser rimligen kan redas ut i efterhand. Datasäkerhetsincidenter, -avvikelser och brott mot datasäkerhet hanteras enligt en hanteringsprocess. Varje arbetstagare i organisationen är förpliktad att göra en anmälan om de upptäcker risker, avvikelser eller övriga dylika situationer som kan äventyra datasäkerheten. Datasäkerhetsteamet ser till att datasäkerhetsöverträdelser registreras, reds ut utan dröjsmål och att de identifierade riskerna hanteras.

När det är fråga om en personuppgiftsincident ska en anmälan göras till tillsynsmyndigheten, och den registrerade ska meddelas i enlighet med lagen och kommunens anvisningar. Dataskyddsombudet i Sibbo kommun är kontaktperson gentemot tillsynsmyndigheten.

5 Riskbaserat förhållningssätt och hantering av datasäkerhetsrisker

I egenskap av personuppgiftsansvarig bedömer kommunen de risker som är förknippade med behandlingen av data och personuppgifter och väljer baserat på den bedömda risknivån de nödvändiga hanterings- och datasäkerhetsåtgärderna.

Genomförandet av datasäkerheten granskas utifrån ett riskbaserat förhållningssätt. Kommunens olika system klassificeras enligt en bedömning om kritiskhet. De kritiska systemens säkerhetsarrangemang kontrolleras regelbundet och deras funktionsduglighet testas vid behov.

Datasäkerheten och metoderna med vilka den hanteras utvecklas ständigt med beaktande av en bedömning och analys av riskerna, praktisk erfarenhet och den allmänna utvecklingen av datasäkerhet.

6 Utbildning och ökad medvetenhet

Datasäkerhetsanvisningar som styr hela kommunen utarbetas i administrativt samarbete. Anvisningarna om datasäkerhet ska 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 uppdaterat. Datasäkerhets- och dataskyddskunnandet påvisas genom genomförd introduktion, olika utbildningsintyg samt genom att följa upp kunnandet. Chefernas tillsynsrättigheter och -skyldigheter omfattar tillsyn över av att dataskyddsanvisningarna följs.

Sibbo kommun förutsätter att alla arbetstagare undertecknar en datasäkerhetsförpliktelse i början av anställningsförhållandet. För att säkerställa personalens kunnande förutsätts att hela personalstyrkan årligen genomgår en utbildning i datasäkerhet och dataskydd. Även förtroendevalda ska utföra datasäkerhets- och dataskyddsutbildningar. Dessutom anordnas årligen utbildning i datasäkerhet och dataskydd för särskilda personalgrupper.

6.1 Kommunikation om datasäkerhetsfrågor

Datasäkerhetspolicyn fastställer gällande datasäkerhetsprinciper. All personal informeras om dokumentet. Den godkända policyn publiceras på kommunens intranät och på kommunens webbplats och personalen informeras om den även på annat sätt. Kommunikation om datasäkerhetsfrågor sköts i allmänhet via datasäkerhetsteam och ledningsgrupperna.

7 Dokumentinformation och versionshistorik

Dokumentinformation	Förklaring
Dokumentnamn	Sibbo kommuns datasäkerhetspolicy
Ägare	Datasäkerhetsteamet
Godkänt av	Kommunstyrelsen
Datum för godkännande	24.10.2022
Dokumentet har uppdaterats	21.7.2022

Version	Datum	Ändringar	Upprättat av
1.0	24.10.2022	Första godkända versionen	Datasäkerhetsteamet