Ängelholms kommun

[Publiceringsdatum]

Policy om informationssäkerhet och personuppgiftsbehandling

för Ängelholms kommun 2021-2031

Dokumentnamn	**Dokumenttyp**	**Fastställd/upprättad**	**Beslutsinstans**
Policy om informationssäkerhet och person-uppgiftsbehandling	Policy	2021-06-21	Kommunfullmäktige
Dokumentansvarig	**Diarienummer**	**Senast reviderad**	**Giltig till**
Säkerhetsenheten	KS 2021/216	Klicka eller tryck här för att ange datum.	2031-12-31

Dokumentinformation
Ängelholms kommuns övergripande principer för informationssäkerhet och personuppgiftsbehandling.
Dokumentet gäller för
Ängelholms kommun, Ängelholm Stadshus AB, AB Ängelholmshem och AB Ängelholmslokaler.

Ängelholm kommuns struktur för styrdokument framgår av Riktlinjer för styrdokument 2020-2024 (beslutad av Kommunstyrelsen den 12 augusti 2020, dnr 2015/864).

V*ision, framtidsförklaring och kommunfullmäktiges mål* *- Visionen ska peka ut en riktning och ett framtida önskvärt tillstånd.*

Plan *- Ett översiktligt och aktiverande dokument.*

Handlingsplan *- Ett detaljerat och aktiverande dokument.*

Policy - Ett översiktligt och normerande dokument.

Policyn ska ange kommunens förhållningssätt till något. Med policy avses grundprincip för en organisations handlande, en övergripande syn på ett sakområde. En policy anger de principer som ska tjäna som vägledning inom det aktuella området och vilka värden som ska beaktas. Den ska konkretiseras med andra styrande dokument, till exempel riktlinjer. Kommunstyrelsen driver och ansvarar för samordning i arbetet med framtagande av en kommunövergripande policy. Kommundirektör, chef för huvuduppdrag och servicestödschef ansvarar på motsvarande sätt för framtagandet av en riktad policy. Policyn beslutas av kommunfullmäktige

Riktlinje *- Ett detaljerat och normerande dokument.*

Innehållsförteckning

1. Sammanfattning av dokumentets sakliga innehåll 3
2. Förhållandet till andra styrdokument 3
3. Om informationssäkerhet och dataskydd 3
4. Mål med informationssäkerhet och dataskydd 4
5. Principer 5
6. Organisation och ansvarsfördelning 6
7. Rapportering och uppföljning 8

1. Sammanfattning av dokumentets sakliga innehåll

Dokumentet syftar till att säkerställa en effektiv styrning och ledning i det systematiska arbetet med informationssäkerhet och behandling av personuppgifter, så kallat dataskydd. Ängelholms kommun ska systematiskt arbeta för att skydda och bevara information som kommunen har att ta ansvar för så att lagstadgade, etiska, verksamhetsrelaterade och avtalade krav upprätthålls. En god informationssäkerhet och personuppgiftshantering bidrar till att skapa förtroende för kommunen och dess bolag hos kommuninvånare och avtalsparter. Det är också en förutsättning för att kunna delta i den digitalisering av samhället som pågår.

Denna policy innehåller Ängelholms kommuns viljeriktning och övergripande principer gällande informationssäkerhet och dataskydd. Policyn med kompletterande riktlinjer ska tillämpas i alla situationer där Ängelholms kommun, Ängelholm Stadshus AB, AB Ängelholmshem och AB Ängelholmslokaler, i fortsättningen benämnda tillsammans som *Ängelholms kommun* eller *kommunen*, hanterar information med eller utan personuppgifter.

2. Förhållandet till andra styrdokument

I Ängelholms kommun finns ett stort antal styrande dokument som kompletterar varandra för att säkerställa att kommunen når sin vision och sina mål. I de fall det föreligger en konflikt mellan olika styrdokument av samma dignitet ska Policy och riktlinjer för informationssäkerhet och personuppgiftsbehandling ha företräde i de fall de ger ett högre skydd för information och registrerade.

3. Om informationssäkerhet och dataskydd

Ängelholms kommuns informationstillgångar består av all information som hanteras i kommunens verksamheter. För att kunna fullgöra de uppdrag som kommunen har på ett effektivt och rättssäkert sätt, samt fullt ut dra fördel av digitaliseringens möjligheter måste informationen hanteras på ett säkert och lagligt sätt.

Informationssäkerhet och dataskydd kräver säkerhetsåtgärder i form av administrativa och organisatoriska åtgärder såsom styrdokument, regler, rutiner och kunskapshöjande insatser. Vidare krävs tekniska åtgärder så som behörighetskontroller, brandväggar och loggning liksom fysiskt skydd i form av exempelvis lås, larm och brandskydd för lokaler. Vilken nivå av skydd som krävs beror på rättsliga krav, kommunens egna prioriteringar och målsättningar samt de förväntningar som samhällets aktörer har kring tillgänglighet och skydd för deras information.

Rättsliga krav på informationssäkerhet och dataskydd återfinns bland annat i offentlighet- och sekretesslagen, arkivlagen, dataskyddsförordningen, lag om informationssäkerhet för samhällsviktiga och digitala tjänster samt Säkerhetsskyddslagen.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre aspekter:

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig
- Riktighet: att information är korrekt, aktuell och fullständig
- Tillgänglighet: att information är åtkomlig och användbar för behöriga.

Utifrån dessa aspekter klassificeras informationen för att kunna bedöma lämpliga skyddsåtgärder.

Information består till stora delar av personuppgifter. Dessa åtnjuter ett särskilt skydd genom dataskyddsförordningen. Regelverket innebär krav på informationssäkerhet men uppställer också ett stort antal rättsliga skyldigheter för personuppgiftsansvariga och rättigheter för dem vars personuppgifter registrerats. Dessa skyldigheter och rättigheter kan inte enbart uppfyllas genom att vidta åtgärder på informationssäkerhetsområdet utan kräver handläggning och uppföljning på annat vis.

4. Mål med informationssäkerhet och dataskydd

Arbetet med informationssäkerhet och skydd för personuppgifter ska ske systematiskt, långsiktigt och med fokus på förebyggande åtgärder. Varje nämnd och styrelse ansvarar för sitt informationssäkerhets- och dataskyddsarbete utifrån intressenter och lagkrav. Varje verksamhet ska inkludera informationssäkerhet och dataskydd i sin verksamhetsplan och beakta att en framgångsrik digitalisering inkluderar ett aktivt informationssäkerhetsarbete för att motverka såväl säkerhetsmässiga som ekonomiska risker när nya tjänster utvecklas, köps in och tas i bruk.

Arbetet med informationssäkerhet och dataskydd ska

- bidra till att Ängelholms kommun når sin vision och sina övergripande planer och mål med verksamheten.
- medföra en robust, säker och tillförlitlig informationshantering med få incidenter
- möjliggöra en trygg, säker och effektiv digitalisering som inte riskerar verksamhetens kontinuitet eller medborgarnas rätt till integritet
- bidra till att leva upp till verksamhetens, medborgares och externa aktörers behov och förväntningar vad gäller tillgänglighet till information samt skydd för personuppgifter och information som omfattas av sekretess.

- efterleva krav i lagar, förordningar, föreskrifter och avtal.

5. Principer

Information är en strategisk tillgång, och tillgång till riktig information är en förutsättning för att fullgöra det uppdrag som kommuner har. Skyddet för personuppgifter är vidare en mänsklig rättighet. Följande principer ska vara vägledande i allt arbete med Ängelholm kommuns information;

- Informationssäkerhet och dataskydd bygger på en helhetssyn som innefattar processer, människor och teknik. Arbetet ska bedrivas resurseffektivt, vilket förutsätter att samtliga aspekter av informationssäkerhet och dataskydd beaktas tidigt i alla initiativ.
- Varje verksamhet ansvarar för sin informationshantering och behöver tillsätta de funktioner som anges i denna policy och tillhörande riktlinjer på ett sådant sätt att de arbetsuppgifter som följer av dokumenten kan genomföras.
- Varje verksamhet ska genomföra informationsklassning, risk- och sårbarhetsanalyser samt vid behov konsekvensbedömningar i enlighet med artikel 35 dataskyddsförordningen.
- Varje verksamhet ska, utifrån lagstiftning och riskerna med informationshanteringen, ställa krav på de aktörer som hanterar informationen, så som digitaliseringsavdelning eller IT-partners, så att lagstiftningen efterlevs och risker hålls på en acceptabel nivå.
- För ett effektivt informationssäkerhetsarbete krävs att all information och alla informationstillgångar, såsom informationssystem och digitala tjänster, har ett tydligt ägarskap. Det vill säga såväl en informationsägare som en systemägare, oavsett om de driftas internt eller externt.
- Arbetet med informationssäkerhet och dataskydd ska bedrivas långsiktigt och förebyggande, och ge förutsättningar att hantera säkerhets- och personuppgiftsincidenter, störningar och eventuella kriser.
- Arbetet med informationssäkerhet och dataskydd ska vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000 med målet att, med utgångspunkt i MSB:s metodstöd[1], skapa ett ledningssystem för informationssäkerhet (LIS).
- Arbetet med informationssäkerhet och dataskydd inom kommunstyrelsen ska vara normerande, stödjande och kontrollerande i förhållande till kommunens övriga verksamheter. Av kommunstyrelsen för ändamålet framtagna gemensamma mallar, rutiner och verksamhetssystem etc. ska användas.

[1] MSBs metodstöd för systematiskt informationssäkerhetsarbete bygger på standarden SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet.

- Beslut avseende inriktning och utformning av åtgärder ska alltid baseras på kommunens egna bedömningar och analyser, med beaktande av särskilt normgivande verksamheter inom informationssäkerhet som t.ex. MSB (Myndigheten för samhällsskydd och beredskap) och SIS (Swedish Standards Institute).
- Medarbetarna är kommunens största tillgång. Det är väsentligt att de löpande får information och utbildning på en adekvat nivå för att kunna utföra sina arbetsuppgifter på ett säkert sätt i enlighet med lagstiftningen och denna policy med tillhörande riktlinjer.
- Att medarbetare vågar anmäla inträffade incidenter är av stor vikt för informationssäkerheten.

6. Organisation och ansvarsfördelning

Huvudprincip - Ansvaret för informationssäkerhet och dataskydd följer verksamhetsansvaret på alla nivåer inom kommunorganisationen. Ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten och dataskyddet inom verksamhetsområdet. Informationssäkerhetsansvariga och övriga som arbetar specifikt med informationssäkerhet, dataskydd, IT-säkerhet eller andra relaterade frågor, utgör stödfunktioner. Nedan beskrivs i ansvaret för ett antal roller. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i tillhörande riktlinjer.

Kommunfullmäktige fastställer denna policy avseende informationssäkerhet och personuppgiftsbehandling som ska gälla för Ängelholms kommun.

Kommunstyrelsen

- ska leda, samordna och följa upp det systematiska arbetet med informationssäkerhet och dataskydd.
- utfärdar de kommunövergripande riktlinjer som kompletterar policyn.
- ansvarar även för att rekrytera eller upphandla dataskyddsombud för nämnder samt i förekommande fall för bolagen.

Nämnder och styrelser

- har det yttersta ansvaret för informationssäkerhet och dataskydd inom respektive verksamhet.
- är personuppgiftsansvariga enligt dataskyddsförordningen för sin verksamhet. Ansvaret kan inte delegeras. Personuppgiftsansvarig ska ge förutsättningar för och kunna visa att dataskyddsförordningen och kompletterande lagstiftning kring

behandling av personuppgifter efterlevs. Ansvaret omfattar att utse och anmäla dataskyddsombud samt säkerställa dataskyddsombudets oberoende ställning.

Kommundirektör, huvuduppdragschefer, servicestödschefer och verkställande direktörer

Har det övergripande ansvaret för:

- att denna policy med tillhörande riktlinjer och instruktioner integreras i organisationens dagliga arbete,
- att relevanta tillämpningsanvisningar/rutiner utfärdas, samt
- att bemanna de funktioner som krävs för att kunna bedriva ett effektivt arbete med informationssäkerhet och dataskydd i enlighet med policyn samt säkerställa representation i kommungemensamma nätverk.

Kommundirektören ansvarar för att det inom kommunstyrelsens verksamhetsområde finns central samordning och stödfunktioner för det systematiska arbetet med informationssäkerhet och dataskydd.

Dataskyddsombudet arbetar självständigt och oberoende med att kontrollera efterlevnaden av dataskyddsförordningen och att ger råd och stöd till de personuppgiftsansvariga och registrerade. Dataskyddsombudets arbetsuppgifter och ställning är reglerad i dataskyddsförordningen.

Medarbetare ansvarar för att följa denna policy och tillhörande riktlinjer. Medarbetare ska aktivt medverka till och förebyggande arbeta för att all information inbegripet personuppgifter hanteras ansvarsfullt, lagligt och korrekt. Medarbetare ansvarar också för att omedelbart anmäla misstänkta incidenter som omfattar personuppgifter.

Digitaliseringsenheten ansvarar för att i alla projekt säkerställa att frågor om informationssäkerhet och dataskydd beaktas i ett tidigt skede, att behovet av säkerhetsåtgärder utreds samt att IT-säkerhet[2] och cybersäkerhet[3], som är betydande och kritiska delar av informationssäkerhetsarbetet, är tillräckliga utifrån informationsklassning och de risker som identifierats. Digitaliseringsenheten ansvarar också för systemförvaltarorganisationen.

[2] Säkerhet i IT-system och IT-infrastruktur

[3] Begreppet, som blivit allt mer etablerat och vedertaget, används ibland annat i Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213) och refererar ofta till säkerhetsåtgärder vid användning av internet såsom skydd mot skadlig kod och IT-attacker.

Informationssäkerhetsansvarig, CISO[4] har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Arbetet sker i samråd med säkerhetschefen och övriga deltagande i kommunens informationssäkerhetsråd.

Central dataskyddssamordnare har det övergripande och strategiska ansvaret att leda, utveckla och samordna arbetet med dataskydd. Arbetet sker i samråd med dataskyddsombudet och CISO samt övriga deltagande i kommunens informationssäkerhetsråd.

Kommunarkivet har enligt Ängelholms kommuns arkivreglemente tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

Upphandlingsenheten ansvarar för att i samtliga upphandlingar ställa krav på leverantörerna utifrån informationssäkerhet, inklusive IT-säkerhet och dataskydd samt tillse att upphandlingen omfattar personuppgiftsbiträdesavtal eller motsvarande avtalshandlingar och klausuler i de fall detta krävs.

7. Rapportering och uppföljning

Kommunstyrelsen ska följa upp det systematiska och strategiska arbetet med informationssäkerhet och dataskydd minst en gång per år.

Nämnder och styrelser

- Ska fastställa mål för verksamheternas arbete med informationssäkerhet och dataskydd och följa upp målet i det interna kontrollarbetet.
- Ska regelbundet följa upp efterlevnaden av denna policy och tillhörande riktlinjer.
- Ska, i rollen som personuppgiftsansvariga, årligen följa upp hur personuppgifter behandlas och hur arbetet med att kvalitetssäkra dataskyddet fortlöper. Inrapporterade personuppgiftsincidenter ska sammanställas och analyseras. I sammanställningen ska det även framgå vilka åtgärder som vidtagits samt förbättringsförslag.

[4] CISO står för Chief information security officer. Titeln används av bland annat Myndigheten för samhällsskydd och beredskap, MSB, och täcker in personer som aktivt arbetar med informationssäkerhet i organisationer i funktioner som informationssäkerhetssamordnare, informationssäkerhetsansvarig eller med liknande arbetsbeskrivning.

Huvuduppdragschefer och servicestödschefer ska årligen rapportera till respektive ansvarig ledning hur åtgärderna/aktiviteterna i styrdokumenten har genomförts, inför framtagande av uppdrag för kommande år.

Dataskyddsombudet ska en gång per år rapportera till personuppgiftsansvarigs högsta förvaltningsnivå gällande arbetet och efterlevnaden av dataskyddslagstiftningen. Om särskilda skäl finns, som exempelvis allvarliga personuppgiftsincidenter, brister eller behov, ska det motivera ytterligare rapporteringar.

CISO ska på uppdrag och anvisning av kommundirektör eller kommunstyrelse rapportera läge och status gällande det övergripande informationssäkerhetsarbetet till kommunledningen. Om särskilda skäl finns, som allvarliga incidenter, brister eller behov, kan det motivera ytterligare rapporteringar till kommunledning, styrelse eller nämnd.

Central dataskyddssamordnare ska följa upp arbetet med dataskydd och på uppdrag och anvisning av kommundirektör eller kommunstyrelse rapportera läge och status gällande det övergripande arbetet med dataskyddsfrågor till kommunledningen. Om särskilda skäl finns, som allvarliga incidenter, brister eller behov kan det motivera ytterligare rapporteringar till kommunledning, styrelse eller nämnd