Alvesta kommun

Alvesta kommun

Informationssäkerhetspolicy

PROGRAM PLAN **POLICY** RIKTLINJE

Beslutat av:	Kommunfullmäktige § 8/2024
Beslutsdatum:	2024-03-19
Gäller från och mer:	2024-03-19
Giltighetstid:	Fyra år från beslutsdatum
Dokumentet gäller för:	Alvesta kommunkoncern
Ansvarig för uppföljning:	Kommunledningsförvaltningen
Diarienummer:	KS 2023-00549 000

Alvesta kommun Postadress: Alvesta kommun, 342 80 Alvesta · Besök: Centralplan 1, 342 80 Alvesta · Tel: 0472-150 00
E-post: kommunen@alvesta.se · Webb: alvesta.se

Alvesta kommun

Datum: 2024-03-19

Dnr: KS 2023-00549 000

Policy

Alvesta kommuns styrdokument

Våra styrdokument kan vara av två huvudtyper, aktiverande och normerande. Aktiverande dokument syftar till förändring och utveckling och anger på så sätt hur vi ska agera för att nå ett visst resultat. Normerande dokument reglerar befintlig verksamhet och talar om hur vi ska förhålla oss till en given situation.

Aktiverande

Aktiverande dokument syftar till förändring och utveckling. De förklarar vad vi vill åstadkomma och utformningen av uppdraget.

Program – Anger långsiktiga ambitioner och viljeinriktningar.

Plan – Anger konkreta åtgärder, tidsramar och ansvar.

Normerande

Normerande dokument berör hur vi utför befintlig verksamhet, till skillnad från aktiverande vars uppgift är att bryta nya vägar.

Policy – Anger kommunens principer eller inriktning i en viss fråga.

Riktlinje – Anger absoluta gränser och skakrav.

Innehållsförteckning

Inledning

Denna policy är det övergripande dokumentet för Alvesta kommuns informationssäkerhetsarbete och omfattar all information som hanteras inom Alvesta kommun, oberoende av var och hur informationen hanteras. Informationssäkerhetspolicyn konkretiseras vidare genom riktlinjer och anvisningar.

Informationssäkerhetspolicyn ska vara väl förankrad i kommunens organisation och policyn med tillhörande riktlinjer och anvisningar ska underlätta för chefer, medarbetare och förtroendevalda att förstå sitt ansvar och sin roll i kommunens informationssäkerhetsarbete.

I denna policy avses med *Alvesta kommun*, hela kommunens organisation och de bolag där kommunen har ett avgörande ägarinflytande.

Syfte

Informationssäkerhetspolicyn redovisar Alvesta kommuns viljeriktning, målsättning, omfattning och ansvar inom informationssäkerhetsarbetet.

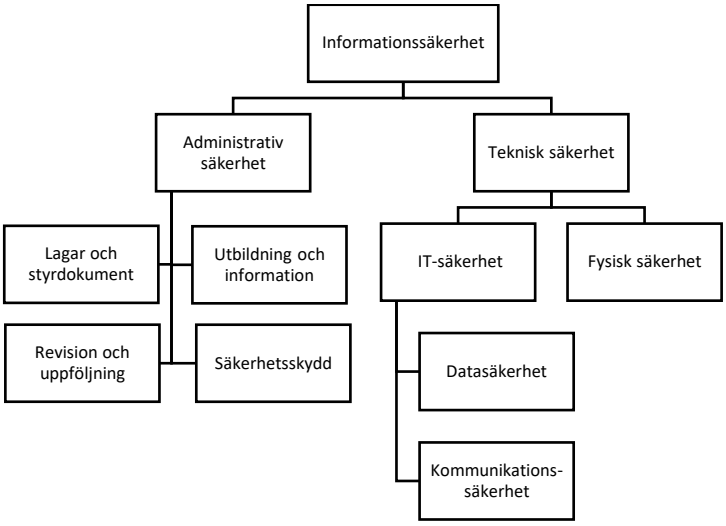
Om informationssäkerhet

Information finns i alla verksamheter och är en av kommunens viktigaste tillgångar. För att uppfylla vad som sägs i lag, och nå en hög kvalitet i verksamheterna, måste därför informationen hanteras på rätt sätt. Informationssäkerhet handlar om att upprätthålla lämpliga rutiner och skydd av information utifrån fyra grundläggande principer:

- **Konfidentialitet**: att informationen inte tillgängliggörs eller avslöjas för obehörig.
- **Riktighet:** att informationen är korrekt och inte är ändrad, manipulerad eller förstörd.
- **Tillgänglighet:** att informationen alltid finns där när den behöver användas.
- **Spårbarhet:** att det tydligt framgår vad som har ändrats, lagts till eller tagit bort i informationen och vem som har gjort förändringen.

Information har i olika grad krav på sig gällande de fyra aspekterna. Kraven kan härledas från rättsliga krav eller från Alvesta kommuns egna målsättningar.

Informationssäkerheten delas in i två olika delar, administrativ säkerhet och teknisk säkerhet. Administrativ säkerhet är till exempel riktlinjer, utbildning och revision. Teknisk säkerhet är till exempel det fysiska skyddet som skyddar en byggnad eller ett serverrum och IT-säkerhet.



Målsättning

Informationssäkerhetsarbetet ska vara en integrerad del i all verksamhet som bedrivs i Alvesta kommun och ska därigenom förebygga och begränsa negativa effekter av oönskade händelser. Informationssäkerheten har inget egenvärde utan ska bidra till att Alvesta kommun:

- Har en robust, säker och tillförlitlig informationshantering.
- Möjliggör ett aktivt medverkande i det digitala samhället.
- Når uppsatta mål gällande exempelvis kvalitet och effektivitet.
- Motsvarar medborgares och externa verksamheters behov och förväntningar.
- Efterlever krav i lagar, föreskrifter och avtal.

Ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunens ledning till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten.

- Kommunfullmäktige uttrycker Alvesta kommuns viljeriktning med informationssäkerhetsarbetet i denna policy.
- Kommunstyrelsen har det strategiska ansvaret för kommunens informationssäkerhet och ansvarar därav för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen ansvarar för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhetsarbetet.
- Kommunstyrelsen, nämnderna och bolagsstyrelserna ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den ska hanteras och av vem den får hanteras.
- Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerhetsarbetet inom sin verksamhet.
- Anställda, förtroendevalda och uppdragstagare ansvarar för att följa Alvesta kommuns policy och riktlinjer för informationssäkerhet. Alla anställda, förtroendevalda och uppdragstagare har ansvar att vara uppmärksamma på brister och incidenter rörande informationssäkerheten och meddela dessa enligt beslutade rutiner.

Grundläggande principer

Kommunstyrelsens arbete med informationssäkerhet ska vara normerande, stödjande och kontrollerande för att kunna identifiera hot, sårbarheter och risker rörande kommunens informationstillgångar. Inom ramen för informationssäkerhetsarbetet ska säkerhetsåtgärder utformas och införas för att reducera dessa risker till en acceptabel nivå.

Informationssäkerheten ska vara en given del vid inköp och upphandling för att säkerställa efterlevnad av god informationssäkerhet utifrån Säkerhetsskyddslagen och dataskyddsslagstiftningen.

Arbetet med informationssäkerhet i Alvesta kommun ska:

- Utgå från informationen men också innefatta processer, människor och teknik.
- Vara systematiskt och bygga på den etablerade standardserien ISO/ICE 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS).
- Löpande ses över och förbättras.
- Vara förebyggande, men också bygga upp förmåga att hantera incidenter, allvarliga störningar och kriser.
- Ta hänsyn till verksamheternas behov.
- Vara väl kommunicerat till verksamheten; alla medarbetare ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och kunna leva upp till denna policy och tillhörande riktlinjer.

Särskilt om dataskydd

Alvesta kommun ska följa dataskyddsförordningen (GDPR) och annan dataskyddslagstiftning i all behandling av personuppgifter, detta innebär bland annat att det ska finnas en laglig grund för varje behandling. De personuppgifter som behandlas ska vara korrekta och det ska vara lätt för utomstående att få insyn i hur behandlingen sker. Insamlade uppgifter får endast behandlas för angivet ändamål och får endast sparas under så lång tid som ändamålet motiverar. Enda undantaget från detta är ytterligare behandling för arkivändamål.

Uppföljning och rapportering

Efterlevnaden av informationssäkerhetspolicyn och riktlinjer ska följas upp regelbundet.

Kommunstyrelsen ska minst en gång per år informera sig om arbetet med informationssäkerhet. Uppföljningen ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten.
- Status och behov gällande utbildning.

- Inträffade incidenter.
- Resultat från genomförda granskningar.
- Aktuella och planerade informationssäkerhetsåtgärder.
- Genomförda riskanalyser.

Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov kan motivera ytterligare rapporteringar.

Gällande dataskyddsarbetet ska respektive personuppgiftsansvarig, minst en gång årligen informera sig om dataskyddsarbetet inom respektive verksamhetsområde.