

## Informationssäkerhetspolicy för Marks kommun

### Om denna informationssäkerhetspolicy

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Marks kommun och dess helägda bolag och kompletterar kommunens övriga gällande styrdokument inom bland annat IT, kommunikation och övrig säkerhet. Alla kommunens verksamheter och medarbetare omfattas av policyn och det finns därför inte utrymme att besluta om lokala rutiner som avviker från policyn.

### Om informationssäkerhet

Information finns i kommunens alla verksamheter och handlar om det vi gör, om vår personal, våra tjänster, vår ekonomi och om det omgivande samhället, kommunens medlemmar, företag, föreningar och så vidare. Information är därför en av kommunens viktigaste tillgångar.

Kommunens informationstillgångar består av all information som finns hos kommunen, inkommer till kommunen eller upprättas av kommunen oavsett var den förvaras, om den är digital, i pappersform eller muntlig.

För att trygga informationsförsörjningen till kommunens alla verksamheter och värna om den personliga integriteten ska kommunen bedriva ett systematiskt och riskbaserat samt långsiktigt informationssäkerhetsarbete som bygger på etablerade standarder och gällande lagstiftning.

För att uppnå en hög kvalitet i vårt arbete måste informationen hanteras på rätt sätt. Informationssäkerhetsarbetet ska upprätthålla rätt skydd för kommunens informationstillgångar utifrån de tre grundläggande principerna **tillgänglighet, riktighet och konfidentialitet**.

Tillgänglighet innebär att informationen är åtkomlig och användbar av den som är behörig att ta del av informationen.

Riktighet innebär att informationen är korrekt, aktuell och fullständig.

Konfidentialitet innebär att information inte tillgängliggörs eller avslöjas för obehörig.

### Mål med informationssäkerhet

Informationssäkerheten syftar till att Marks kommun ska nå sina övergripande visioner, strategier och mål. Marks kommun ska nå och upprätthålla en informationssäkerhet som:

- Innebär en säker, robust och tillförlitlig informationshantering

<b>Dokumenttyp</b> Policy	<b>Fastställt av</b> Kommunfullmäktige	<b>Beslutsdatum</b> 25-09-18 § 127	<b>Giltig till</b> Tills vidare
<b>Dokumentansvarig</b> Säkerhet- och beredskapschef	<b>Gäller för</b> Kommunen och dess helägda bolag	<b>Granskad/ reviderad</b> -	<b>Diariennr.</b> KS 2023 485

- Möjliggör ett aktivt medverkande i och bidragande till det digitala samhället
- Bidrar till att uppsatta mål nås avseende exempelvis kvalitet, effekt och personlig integritet
- Motsvarar kommunmedlemmarnas och externa verksamheters behov och förväntningar
- Uttrycks i aktuella styrdokument som policy och riktlinjer
- Efterlever krav i lagar, förordningar, föreskrifter, standarder och avtal
- Bidrar till att upprätthålla kommunmedlemmarnas förtroende för kommunens verksamheter.

### Principer för informationssäkerhetsarbete

Informationssäkerhetsarbetet i Marks kommun ska utgå från följande principer:

- Informationssäkerhetsarbetet ska bedrivas systematiskt, långsiktigt och riskbaserat. Det systematiska informationssäkerhetsarbetet ska bedrivas strukturerat och kontinuerligt.
- All information ska ha en ägare.
- Riktlinjer och rutiner för informationssäkerheten i kommunen ska utgå från förekommande policy, aktuella standarder och gällande lagstiftning, inkluderande men ej begränsat till NIS-lagen och ISO 27000-standarderna.
- Kommunen ska klassa informationen enligt vald klassningsmodell.
- Krav på spårbarhet ska finnas i överenskommen omfattning i all informationshantering samtidigt som den personliga integriteten ska värnas.
- Risker som kan påverka kommunens informationssäkerhet ska identifieras, analyseras, åtgärdas och följas upp.
- Konsekvensbedömning ska genomföras enligt Artikel 35 Dataskyddsförordningen (GDPR) om det kan finnas en risk för att behandlingen av information kan påverka den registrerades rättigheter och friheter.
- All systemförvaltning samt både intern och extern drift av IT-miljön ska bedrivas utifrån kommunens regelverk och de specifika krav som ställs av verksamheten genom bland annat informationsklassning och riskanalyser.

<b>Dokumenttyp</b> Policy	<b>Fastställd av</b> Kommunfullmäktige	<b>Beslutsdatum</b> 25-09-18 § 127	<b>Giltig till</b> Tills vidare
<b>Dokumentansvarig</b> Säkerhet- och beredskapschef	<b>Gäller för</b> Kommunen och dess helägda bolag	<b>Granskad/ reviderad</b> -	<b>Diariennr.</b> KS 2023 485

- Åtkomst till information, behörighetsstyrning, ska ges efter tydliga riktlinjer, tydliga ansvarsförhållanden, enhetliga metoder och ska följas upp regelbundet.
- Marks kommun ska ha tydliga rollbeskrivningar och dokumenterade rutiner för ansvarsfördelning inom informationssäkerhetsområdet.
- Vid kontinuitetsplanering ska åtgärder för att säkerställa tillgång till information vid en krissituation vidtas.
- En process för incidentrapportering och incidenthantering avseende riktighet, tillgänglighet och konfidentialitet ska finnas för att mildra effekter, förhindra upprepande och underlätta återgång till verksamhet på normal nivå.
- Hotbilden mot informationstillgångarna ska analyseras och bevakas.

## Roller och ansvar

Roller och ansvar utgår från en grundläggande ansvarsfördelning för informationssäkerhetsarbetet och följer befintliga ansvarsförhållanden enligt gällande delegationsordning.

Kommunfullmäktige är ytterst ansvarig för informationssäkerhetsarbetet i kommunen och uttrycker sin viljeriktning i den här policyn.

Kommunstyrelsen ska samordna och följa upp och kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta, utveckla och följa upp kommunens riktlinjer för informationssäkerhet.

Nämnder och kommunala bolag ansvarar för informationssäkerheten i den egna verksamheten och för att säkerställa den egna förvaltningens förmåga att arbeta med och upprätthålla en god informationssäkerhet.

Medarbetarna har ansvar för att följa kommunens informationssäkerhetspolicy, riktlinjer för informationssäkerhet och övriga delar av ledningssystemet för informationssäkerhet. Man har som medarbetare också ansvar för att vara uppmärksam på brister och incidenter rörande informationssäkerheten och rapportera i utpekade system och enligt gällande rutin.

Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom den egna verksamheten. Det åligger varje verksamhetsansvarig att tillse att medarbetarna har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet ska uppnås i verksamheten.

Informationsägaren ansvarar för att samtliga krav i informationssäkerhetspolicy och riktlinjer för informationssäkerhet kopplade till informationsmängden uppfylls. En viktig del i ansvaret är

<b>Dokumenttyp</b> Policy	<b>Fastställd av</b> Kommunfullmäktige	<b>Beslutsdatum</b> 25-09-18 § 127	<b>Giltig till</b> Tills vidare
<b>Dokumentansvarig</b> Säkerhet- och beredskapschef	<b>Gäller för</b> Kommunen och dess helägda bolag	<b>Granskad/ reviderad</b> -	<b>Diariennr.</b> KS 2023 485

att besluta om objektets informationssäkerhetsnivå genom att klassning och riskanalys sker i enlighet med kommunens modell för klassning och riskanalys. Vem som är informationsägare ska kunna utläsas av systemdokumentationen som kommunens systemförvaltningsmodell ställer krav på.

Kommunstyrelsen ansvarar för att den tekniska IT-säkerheten inom Marks kommuns IT-infrastruktur - avseende klienter, nätverk och server-/applikationsdrift är tillräcklig och är anpassad utifrån verksamhetens krav såväl som legala krav samt denna policy och riktlinjerna för informationssäkerhet.

Kommunstyrelsen ansvarar för att den tekniska IT-säkerheten kontinuerligt anpassas utifrån en förändrad krav- och behovsbild.

### Uppföljning och rapportering

Efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet ska följas upp regelbundet.

Informationssäkerhetssamordnaren ska årligen rapportera läge, status och planering gällande informationssäkerheten i kommunen till kommunstyrelsen och kommundirektören. Särskilda skäl, incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

<b>Dokumenttyp</b> Policy	<b>Fastställt av</b> Kommunfullmäktige	<b>Beslutsdatum</b> 25-09-18 § 127	<b>Giltig till</b> Tills vidare
<b>Dokumentansvarig</b> Säkerhet- och beredskapschef	<b>Gäller för</b> Kommunen och dess helägda bolag	<b>Granskad/ reviderad</b> -	<b>Diariennr.</b> KS 2023 485