

Informationssäkerhetspolicy 2026 - 2030

-  Mål
-  Taxa
-  Reglemente
-  Policy
-  Plan
-  Delegationsordning
-  Riktlinje

Dokumentnamn	Dokumenttyp	Fastställd	Beslutsinstans
Informationssäkerhetspolicy	Policy	2026-04-27 § 54	KF
Dokumentansvarig	Diarienummer	Reviderad	Giltig till
Informationssäkerhetssamordnaren	KS 2026/110	--	2030
Dokumentinformation			
Dokumentet visar på Markaryds kommuns vilja och avsikt med informationssäkerhet, vilket handlar om att rätt information ska finnas tillgänglig för rätt person vid rätt tid.			
Dokumentet gäller för			
Markaryds kommun			

Innehållsförteckning

1. Syfte och mål	1
2. Genomförande.....	1
3. Generell informationsklassning	1

1. Syfte och mål

Denna policy visar på Markaryds kommuns, dess nämnder, styrelser och bolags vilja och avsikt med informationssäkerhet, det vill säga att rätt information ska finnas tillgänglig för rätt person vid rätt tid och att informationen inte ska förloras eller förvanskas. För att korrekt hantera de informationstillgångar och tjänster som berör det kommunala arbetet och kommunens medborgare ska kommunens informationshantering genomföras systematiskt, riskbaserat och effektivt. Detta mål gäller för all information oberoende av typ, form eller miljö den förekommer i, såväl digitalt som manuellt behandlad.

2. Genomförande

Behovet av informationssäkerhet växer i samband med skapande och hantering av olika informationstillgångar och tjänster inom kommunens verksamhet. Markaryds kommun är mån om att dessa tillgångar och tjänster hanteras korrekt och att hanteringen uppfyller kraven enligt de nedan fyra aspekterna. Genom konsekvensanalyser ska ett tolerabelt skydd identifieras. Skyddsåtgärderna ska vara lämpliga och proportionella utifrån ett allriskperspektiv.

Brister i informationssäkerhetsarbetet, som exempelvis att information förloras, förvanskas eller stjäls, kan leda till konsekvenser för såväl organisation som individ. Konsekvenser som kan ge negativ påverkan på förtroendet, generera föreläggande, anmärkning eller sanktionsavgifter. Därför är det av stor betydelse att tillgångarna skyddas. Ansvaret för informationssäkerheten följer verksamhetsansvaret. Alla chefer, medarbetare och förtroendevalda ansvarar för att denna policy och tillhörande riktlinjer, anvisningar och instruktioner följs vid hantering av kommunens informationstillgångar. Allra minst ska all information genomgå generell informationsklassning.

3. Generell informationsklassning

Genom konsekvensanalys identifieras informationen enligt de fyra aspekterna nedan och därefter bedöms klassificeringsnivåerna (K1-5) proportionerligt i förhållande till risken:

1. alla medarbetare ska ha tillgång till den information som de behöver för att utföra sina arbetsuppgifter och åtaganden (**tillgänglighet**),
2. informationen ska vid varje tillfälle vara korrekt och informationsresurserna ska säkerställa att informationen inte kan förvanskas genom obehörig eller felaktig hantering (**riktighet**),
3. informationen och informationsresurserna ska alltid vara skyddade mot obehörig åtkomst (**konfidentialitet**), och
4. det ska i efterhand gå att visa vad som har hänt, när det hände och vem som har gjort vad (**spårbarhet**).

Klassificeringsnivåerna avgör på vilken lagringsyta som informationen ska placeras, enligt följande exempel:

Klassificeringsnivå	Informationsklass	Lagringsyta
K5	Säkerhetsskyddsklassifierad information rörande Sveriges säkerhet	Fristående dator för hemlig information (H-dator)
K4	Extra skyddsvärd/Mycket känslig	Verksamhetssystem
K3	Skyddsvärd/Känslig	Verksamhetssystem
K2	Intern	Flertalet ytor
K1	Allmän info	Webb

Detaljerad information om tillvägagångssätt återfinns i riktlinjer för informationssäkerhet.