MARKARYDS KOMMUN

Informationssäkerhetspolicy

MARKARYDS KOMMUN

Dokumentnamn	Dokumenttyp	Fastställd	Beslutsinstans
Informationssäkerhetspolicy	Policy	2020-02-04	KF
Dokumentansvarig	**Diarienummer**	**Reviderad**	**Giltig till**
Informationssäkerhetssamordnare	2020/20	2024-03-01	2028-03-01
Dokumentinformation	Syftet med dokumentet är att förtydliga ansvaret och fokusområdena inom informationssäkerhet.		
Dokumentet gäller för	Markaryds kommun		

MARKARYDS KOMMUN

Innehåll

Inledning

Behovet av informationssäkerhet växer i samband med skapande och hantering av olika informationstillgångar och tjänster inom kommunens verksamhet. Markaryds kommun är måna om att dessa tillgångar och tjänster hanteras korrekt och därmed uppfyller kraven för tillgänglighet, riktighet och konfidentialitet.

Brister i informationssäkerhetsarbetet kan leda till konsekvenser, till exempel att information förloras, förvanskas eller stjäls. För Markaryds kommun kan det även innebära negativ påverkan på förtroendet för kommunen. Därför är det av stor betydelse att tillgångarna skyddas.

Definitioner

Informationssäkerhet kan beskrivas kortfattat i enlighet med följande kravområden:

Tillgänglighet - Att informationen är tillgänglig i förväntad utsträckning, för behöriga och inom önskad tid.
Riktighet - Att informationen är skyddad mot oönskad förändring eller borttag.
Konfidentialitet - Att informationen inte delges för obehöriga.
Spårbarhet – Att händelser som berör information kan spåras.

Syfte

Denna informationssäkerhetspolicy beskriver kommunens tillvägagångssätt för att korrekt hantera de informationstillgångar och tjänster som berör kommunen och dess invånare. All information som är av värde för kommunen avser en informationstillgång. Detta gäller för information oberoende av typ, form eller miljön den förekommer i. Syftet är att framföra kommunens avsikter, att de berörda informationstillgångar och tjänster behandlas i enlighet med uppsatta mål som beskrivs i nästa avsnitt.

Mål

Informationssäkerhetspolicyn omfattar hela Markaryds kommun och innehåller följande mål:

Mål	Beskrivning
Informationssäkerhet	Arbete med informationssäkerhet sker naturligt och integreras i verksamheten. Informationssäkerhetsarbetet ska följa etablerade ISO standarder och vägledningar från Myndigheten för samhällsskydd och beredskap. Kunskap gällande hur informationssäkerhet säkerställs, upprätthålls och förbättras, ska finnas och utvecklas fortlöpande.
Informationsklassning	Alla informationstillgångar och tjänster klassificeras utifrån sitt värde (för kommunen, invånarna) och revideras löpande. KLASSA-verktyget ska användas för att uppnå målet.
Risk- och incidenthantering	Risker och incidenter avser händelser som medför/resulterar i negativ konsekvens. Risker och incidenter som påverkar informationstillgångar tas fram och bedöms genom riskanalyser. En prioriteringsordning för att påbörja riskanalyser sker baserat på resultatet från informationsklassningen.
Kontinuitetshantering	Kontinuitetshantering av informationssäkerhet ska planeras, införas och granskas för att klara av svåra situationer som exempelvis under en kris eller katastrof. Kontinuitetsplan ska tas fram för de mest kritiska/viktiga informationstillgångar och tjänster inom kommunen.
Uppföljning och revidering	Informationssäkerhetsarbetet och tillhörande säkerhetsåtgärder följs upp och revideras vart fjärde år.

Tabell 1: Mål

Ansvarsförhållande

Ansvarsförhållanden listas i följande tabell och avser olika ansvarsområden för informationssäkerhet inom Markaryds kommun.

Kommunfullmäktige	Kommunens högsta beslutsorgan.
Kommunstyrelsen	Leder och samordnar arbetet inom kommunen. Har det yttersta ansvaret för Markaryds kommun och ser till att informationssäkerhetspolicyn fastställs och efterlevs.
Dataskyddsombud	Stödjer kommunens tjänstepersoner i informationssäkerhetsrelaterade frågor kopplat till rättsliga krav.
Informationssäkerhetssamordnare	Samordnar informationssäkerhetsarbetet. Ansvarar även för att driva risk- och incidentprocesser framåt.
IT-säkerhetschef	Driver IT-infrastrukturen och tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet.
Respektive nämnd	Varje nämnd ansvarar för att upprätthålla informationssäkerheten inom sitt verksamhetsområde.
Medarbetare	Alla medarbetare ska följa informationssäkerhetspolicyn i sitt arbete och rapportera brister eller fel (gällande informationshantering) enligt fastställda rutiner.

Tabell 2: Ansvarsförhållande

Relaterade dokument

Det finns relaterade dokument till informationssäkerhetspolicyn. Dessa förmedlar specifika regler, riktlinjer och rutiner, angående hur informationssäkerhetspolicyn ska efterlevas. Dokumenten finns på intranätet under sidan med GDPR samt nedanstående riktlinjer.

- Riktlinjer för identifiering
- Riktlinjer för internetanvändning
- Riktlinjer för e-post hantering
- Riktlinjer för hantering av personuppgifter
- Riktlinjer för mobiltelefoni

Avvikelser

Avvikelser ifrån denna informationssäkerhetspolicy eller vidhängande regelverk, ska rapporteras till informationssäkerhetssamordnaren.