

Informationssäkerhetspolicy för Vännäs kommun



Informationssäkerhetspolicy	Datum för beslut: 2020-05-18
Kommunstyrelseförvaltningen	Reviderad:
Beslutsinstans: KS § 64	Giltig till: Tills vidare

Innehåll

1.	Om denna informationssäkerhetspolicy	3
2.	Inledning	3
3.	Syfte	3
4.	Struktur för informationssäkerhetsarbetet	4
5.	Mål för informationssäkerhet i Vännäs kommun	4
6.	Principer och arbetssätt	5
7.	Roller och ansvar	5

1. Om denna informationssäkerhetspolicy

Informationssäkerhetspolicyn är ett dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Vännäs kommun, och kompletterar kommunens övriga styrdokument inom säkerhetsområdet. Hela kommunkoncernen omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

2. Inledning

Informationssäkerhet är de åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs. Informationen som ska skyddas kan vara tryckt på papper, vara lagrad elektroniskt, överförs med post eller med elektroniska hjälpmedel, visas på film eller yttras i en konversation.

Inom Vännäs kommun hanterar vi stora mängder av information som är viktiga för kommuninvånare, medarbetare, företag och organisationer. Att hantera sådan information på ett korrekt sätt skapar tillit och förtroende. Att den även är tillgänglig då informationen behövs samt att känslig information skyddas leder till en trygghet för alla inom kommunens verksamheter, både internt och externt. Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning.

En väl utvecklad och integrerad informationssäkerhet bidrar till att etablera effektiv och ändamålsenlig informationshantering, vilket skapar förtroende både inom och utanför organisationen och direkt bidrar till att:

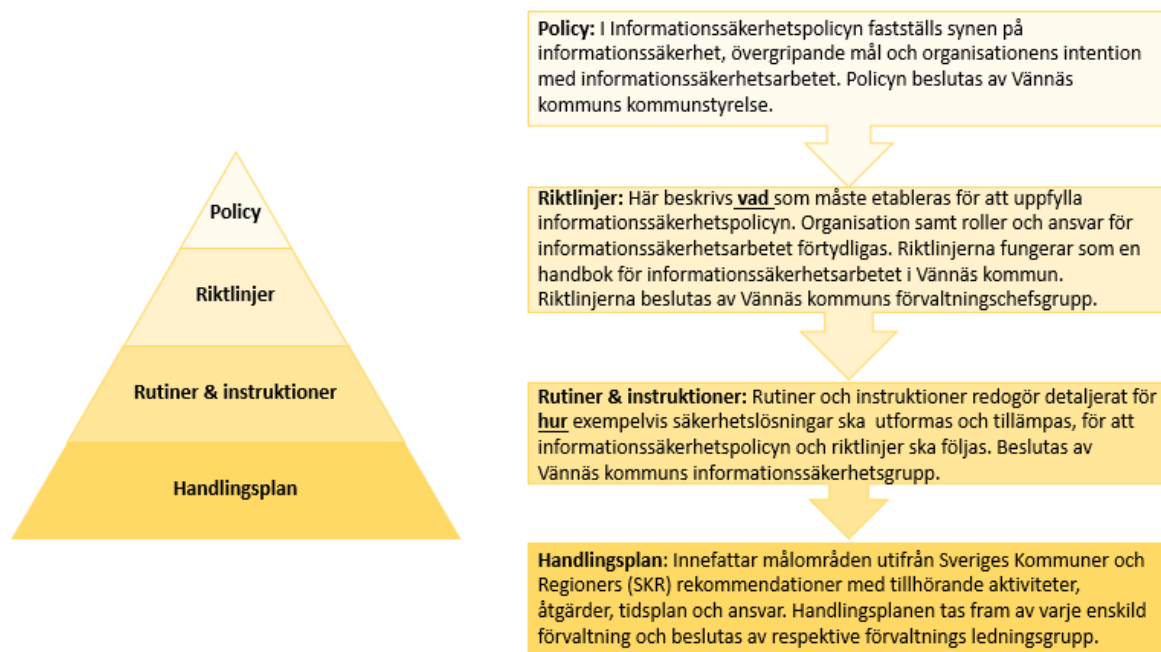
- Möjliggöra digitaliseringssatsningar och underlätta transformering
- Undvika incidenter – bygga ett skydd mot it-attacker och läckage av personuppgifter
- Säker verksamhetsstyrning
- Bevara förtroende mot medborgare
- Införa en metodik och ett arbetssätt för att efterleva lagstiftning och löpande uppföljning

3. Syfte

Informationssäkerheten syftar till att säkerställa informationens konfidentialitet, riktighet och tillgänglighet. Samt att kommunen uppfyller gällande lagkrav.

- **Konfidentialitet** innebär att säkerställa att enbart behöriga personer får ta del av informationen.
- **Riktighet** innebär att informationen ska vara korrekt och inte manipulerad eller förstörd.
- **Tillgänglighet** innebär att informationen måste vara tillgänglig när den behövs.

4. Struktur för informationssäkerhetsarbetet



Figur 1: Vännäs kommuns regelverk för informationssäkerhet.

5. Mål för informationssäkerhet i Vännäs kommun

De övergripande målen med informationssäkerhetsarbetet är att:

- Skydda kommunens informationstillgångar¹
- Information alltid finns tillgänglig för de som är behöriga
- Information inte finns eller görs tillgänglig för obehöriga
- Information inte utnyttjas på otillåtet sätt
- Information skyddas mot oavsiktlig eller avsiktlig förvanskning
- Alla anställda har kunskap om informationssäkerhet och medverkar till förbättringar och utveckling av informationssäkerhet

De övergripande målen bryts ner till mer kortsiktiga mål för respektive förvaltning i en handlingsplan.

¹ Informationstillgång: Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t ex. rykte).

6. Principer och arbetssätt

Vännäs kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Viktiga förmågor i informationssäkerhetsarbetet är att kunna identifiera hot, sårbarheter och risker rörande Vännäs kommuns informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Som stöd för ett systematiskt informationssäkerhetsarbete ska en handlingsplan upprättas för respektive förvaltning. Handlingsplanen ska innehålla Sveriges Kommuner och Regioners (SKR) rekommenderade målområden med tillhörande aktiviteter, tidsplaner, ansvar och uppföljning. Handlingsplanen revideras var tredje år och följs upp kontinuerligt.

Målområden i handlingsplan:

1. Hur ledningen ska leda och styra
2. Riskhantering/identifiering
3. Informationsklassning. Klassning ska utföras i SKR:s verktyg KLASSA
4. Incident-/avvikelsehantering
5. Kontinuitetsplan
6. Utbildning och medvetandehöjande insatser
7. Upphandling
8. Behörighetskontroll. Informationssäkerhet i processen för nyanställning, förändring och avslut av anställning.
9. Uppföljning

I övrigt ska arbetet med informationssäkerhet inom Vännäs kommun:

- Bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik
- Vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000
- Löpande ses över och förbättras, eftersom Vännäs kommun och dess omvärld, inklusive hotbild, är under ständig förändring

7. Roller och ansvar

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

Kommunens informationssäkerhetssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i *Riktlinjer för informationssäkerhet*.

Kommunstyrelsen har det yttersta ansvaret för informationssäkerhet.

Kommunchef/VD har det övergripande ansvaret för informationssäkerhet.

Förvaltningschef/VD är informationsägare och systemägare. Detta innebär bland annat ansvar för att informationen klassificeras och att beslutade insatser i enlighet med handlingsplanen genomförs.

Systemförvaltare är den eller de personer i berörda verksamheter som har ansvaret för den dagliga användningen av det digitala verksamhetsstödet.

Informationssäkerhetssamordnare har det övergripande och strategiska ansvaret att utveckla och samordna informationssäkerhetsarbetet.

Personuppgiftsansvariga är kommunstyrelsen, övriga nämnder och bolagsstyrelser i kommunen. Dessa är ansvariga för behandling av personuppgifter.

Dataskyddsbud kontrollerar att personuppgifter behandlas på ett korrekt sätt i verksamheten.

Samtliga **medarbetare och förtroendevalda** har ansvar och skyldighet att:

- Efterleva och arbeta utifrån gällande regler och rutiner i *Informationssäkerhetspolicyn* och *Riktlinjer för informationssäkerhet* med tillhörande dokument.
- Rapportera oönskade händelser
- Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten och bidra till dess utveckling och förbättring.