

Informationssäkerhetspolicy för Vännäs kommun



Informationssäkerhetspolicy	Datum för beslut: 2020-05-18
Kommunstyrelseförvaltningen	Reviderad: 2023-11-20
Beslutsinstans: KS § 129	Giltig till: Tills vidare

Innehåll

1.	Inledning	3
2.	Om informationssäkerhet	3
3.	Mål med informationssäkerhet.....	5
4.	Principer och arbetssätt	5
5.	Roller och ansvar	6

1. Inledning

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Vännäs kommun, och kompletterar kommunens övriga styrdokument inom bland annat IT, kommunikation och övrig säkerhet. Kommunstyrelsen i Vännäs kommun beslutar om Informationssäkerhetspolicyn, för mindre icke-principiella förändringar kan beslut ske i kommunstyrelsens arbetsutskott.

Policyn är ett centralt styrdokument som redovisar kommunens och dess bolags viljeinriktning och mål inom informationssäkerhet och dataskydd samt hur ansvaret i dessa frågor är fördelat. Policyn är styrande för informationssäkerhets-, IT-säkerhets-, och dataskyddsarbetet i Vännäs kommun. Riktlinjer för informationssäkerhet kompletterar och konkretiserar denna policy. Ytterligare kan mer detaljerade instruktioner förekomma och tas fram vid behov som ger verksamheterna stöd i informationssäkerhetsarbetet och bättre förutsättningar för att upprätthålla tillräcklig informationssäkerhet.



Figur 1. Styrande dokument för informationssäkerhet och dataskydd i Vännäs kommun.

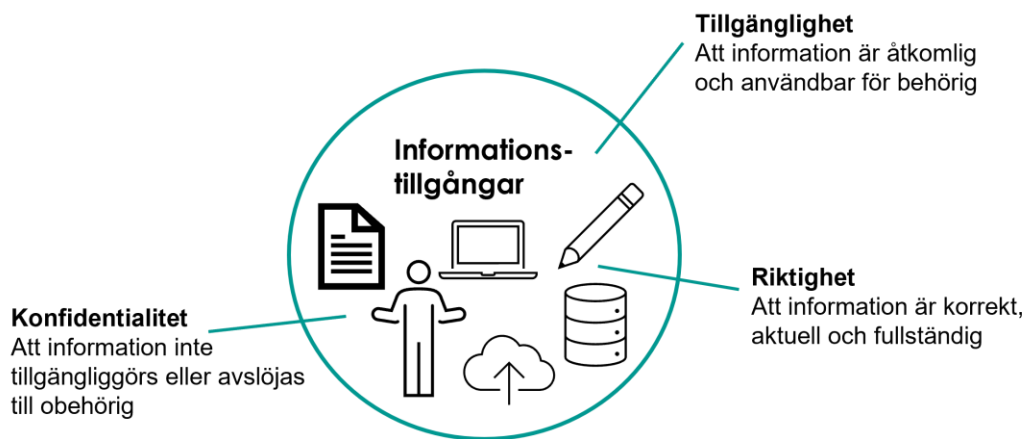
Alla verksamheter omfattas av policyn, vilket medför att det inte finns utrymme för lokala avvikelser. Policyn utgör grunden för det systematiska arbetet med informationssäkerhet och ska även tillgodose de krav på informationssäkerhet som ingår i dataskyddsförordningen.

För information som faller under säkerhetsskyddslagen (information som är av vikt för Sveriges säkerhet) har Vännäs kommun en säkerhetsskyddspolicy. Informationssäkerhetspolicy och säkerhetsskyddspolicy kompletterar varandra.

2. Om informationssäkerhet

Information finns i alla kommunens verksamheter och handlar om allt det vi gör, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med medborgare, företag, föreningar osv. Information är därför i sig en av kommunens viktigaste tillgångar.

För att nå tillräcklig säkerhet och en hög kvalitet för vårt arbete måste information hanteras på rätt sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information utifrån de tre aspekter: **Konfidentialitet, riktighet och tillgänglighet.**

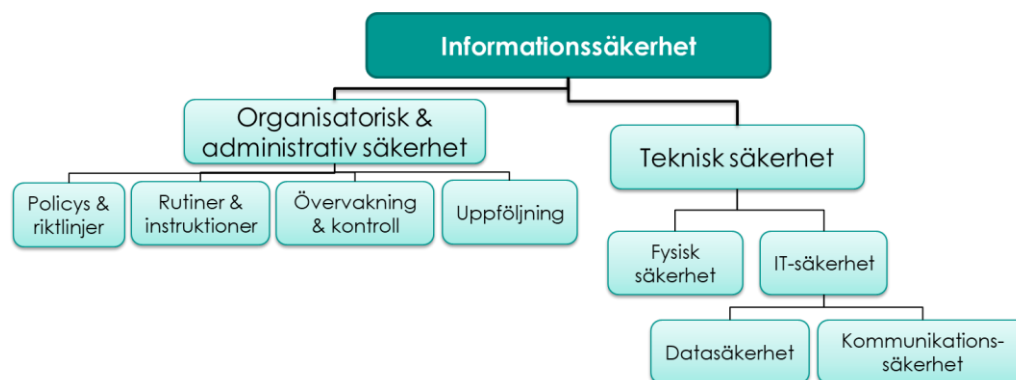


Figur 2. Tre aspekter inom informationssäkerhet; att informationstillgångar ska vara konfidentiella, riktiga och tillgängliga. Informationstillgång är: Allt som innehåller information och allt som bär på informationen.

Information har i olika grad krav på sig gällande de tre aspekterna. Kraven kan härledas från rättsliga krav eller från Vännäs kommuns egna målsättningar. I dataskyddslagstiftningen som styr hur vi får behandla information innehållande personuppgifter, ställs också krav på informationssäkerheten. Dessutom har medborgare, företag och andra aktörer i vår omvärld, behov och förväntningar som ställer krav på vår informationssäkerhet.

Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oavsett hur information lagras, bearbetas och delas. Information kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Informationssäkerhet består av organisatorisk- och administrativ säkerhet och teknisk säkerhet. Enkelt beskrivet har den organisatoriska och administrativa säkerheten fokus på styrning, människor och beteende. Medan den tekniska säkerheten som delas in i två delar, fysisk säkerhet och IT-säkerhet har fokus på tekniskt skydd för IT, föremål och lokaler.



Figur 3. Informationssäkerhetens olika delar.

Brister i informationssäkerhet kan leda till risk för liv och hälsa, hot mot den personliga integriteten samt leda till negativ ekonomisk påverkan och att förtroendet för kommunen skadas. Sammantaget har vi stora krav på

informationssäkerhet och därför är systematik och en fast styrning nödvändig för att upprätthålla säkerhet och kvalitet.

3. Mål med informationssäkerhet

De övergripande målen med informationssäkerhetsarbetet i Vännäs kommun är att:

- Skydda kommunens informationstillgångar¹
- Skydda personuppgifter enligt General Data Protection Regulation (GDPR)
- Information alltid finns tillgänglig för de som är behöriga när den behövs
- 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 att upprätthålla, förbättra och utveckla informationssäkerheten

4. Principer och arbetssätt

Vännäs kommun ska arbeta med informationssäkerhet systematiskt och på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot kommunens verksamheter vara stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Vännäs kommuns informationstillgångar¹ samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Vännäs kommun ska:

- Bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik
- Efterleva krav i lagar, förordningar, föreskrifter och avtal.
- 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.
- Säkerställa rätt nivå av skydd vad gäller tillgänglighet, riktighet och konfidentialitet utifrån en fastställd organisationsgemensam modell för informationsklassning
- Vara förebyggande och proaktivt, samtidigt även ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa.
- Vara väl kommunicerat till verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy och underliggande riktlinjer för informationssäkerhet och instruktioner.
- Möjliggöra en hållbar digitalisering
- Främja och utveckla kommunens säkerhetskultur

¹ Informationstillgång: Allt som innehåller information och allt som bär på informationen. Organisationens information, och även de resurser som hanterar den, exempelvis papper, mjukvara, hårdvara.

- Motsvara medborgares, medarbetares och externa verksamheters behov och förväntningar

5. 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, dataskydd/GDPR eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

Informationssäkerhet är allas ansvar, regelverk med policy och riktlinjer gäller samtliga medarbetare i Vännäs kommun. Verksamhetsansvariga och alla chefer har en utökad skyldighet att se till att medarbetarna känner till regelverket och att regler och lagar följs för informationssäkerhet inom den egna verksamheten.

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

Kommunstyrelsen har det yttersta ansvaret för informationssäkerhetsarbetet i Vännäs kommun. Kommunstyrelsen fastställer övergripande mål och riktning för informationssäkerhet genom kommunövergripande informationssäkerhetspolicy.

Nämnd och bolagsstyrelse, varje nämnd och bolagsstyrelse ansvarar för informationssäkerheten inom sitt verksamhetsområde. Nämnd och bolagsstyrelse är informationsägare och systemägare.

Kommunchef /VD är den tjänsteperson som har det övergripande och yttersta ansvaret för informationssäkerhetsarbetet. Kommunchef/VD ska säkerställa att rätt förutsättningar finns för att uppfylla målen enligt Vännäs kommuns informationssäkerhetspolicy.

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetsansvarig ansvarar för att all informationshantering inom egna verksamheten sker i enlighet med lagar och fastställda styrdokument.

Förvaltningschef/VD har ett delegerat uppdrag som informationsägare och systemägare från varje nämnd/styrelse. Varje förvaltningschef/VD är ansvarig för informationssäkerheten inom respektive förvaltning eller bolag.

Säkerhetsskyddschef ansvarar och samordnar informationssäkerheten i verksamhet som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen.

Informationsägare ansvarar för informationstillgångarna och är därmed även riskägare. Informationsägare är nämnd eller bolag, nämnden/styrelsen delegerar till

en funktion att verkställa ansvaret. I Vännäs kommun ska förvaltningschef eller verkställande direktör som svarar mot nämnd/styrelse anges som informationsägare. Informationsägare har det övergripande ansvaret för informationen.

Systemägare är nämnd eller styrelse där systemet används, nämnden/styrelsen delegerar till en funktion att verkställa ansvaret. I Vännäs kommun ska förvaltningschef eller verkställande direktör som svarar mot nämnd/styrelse anges som systemägare. Förvaltningschef/VD kan delegera rollen som systemägare till annan medarbetare i sin verksamhet som har ekonomiskt ansvar och mandat att fatta beslut för systemet. Systemägare har det övergripande ansvaret för systemet.

Informationssäkerhetssamordnare har det övergripande ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet i kommunen.

IT-chef har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. IT-chefen har ett särskilt ansvar för den tekniska IT-säkerheten.

IT-säkerhetsansvarig ansvarar för att upprätthålla, leda, utveckla och samordna arbetet med IT-säkerheten i Vännäs kommuns IT-miljö.

Personuppgiftsansvariga är kommunstyrelsen, övriga nämnder och bolagsstyrelser i kommunen. Dessa är ansvariga för all behandling av personuppgifter inom sitt verksamhetsområde. Kommunstyrelsen ska utse dataskyddsbud, vilket är delegerat till kommunchef och biträdande kommunchef.

Dataskyddsbud har en stödjande, vägledande roll i organisationen och ska tillse efterlevnad av gällande dataskyddslagstiftning. Är kontaktperson för de registrerade, för den egna organisationen och för tillsynsmyndigheten.

Informationssäkerhetsombud är utsedda av respektive förvaltningschef/avdelningschef/VD och ska stödja och samordna arbetet med informationssäkerhet och dataskydd/GDPR inom sin förvaltning/avdelning/bolag.

Medarbetare, förtroendevalda och extern personal har ansvar och skyldighet att:

- Efterleva och arbeta utifrån policy, riktlinjer, instruktioner, lagar och regler för informationssäkerhet.
- Rapportera oönskade händelser – genom incidentrapportering.
- Ha den kunskap som krävs för att förstå sitt ansvar för informationssäkerhet.
- Upprätthålla informationssäkerheten och bidra till dess utveckling och förbättring.