VILHELMINA KOMMUN

VUALTJEREN TJÏELTE

Policy för informationssäkerhet

Ledningssystem för informationssäkerhet

Kommunstyrelsens förvaltning / Beredskapsfunktionen 2026-01-01

Dokumenttyp	**Dokumentansvarig**	**Beslutsinstans**	**Diarienummer**
Policy	CISO	Kommunfullmäktige	xxxx
Upprättad av	**Ansvarig verksamhet**	**Gäller från**	**Revideras senast**
Informationssäkerhetssamordnare/ML	Beredskapsfunktionen	2026-01-01	2029-09-01

VILHELMINA KOMMUN
VUALTJEREN TJÏELTE

Innehållsförteckning

Innehåll

VILHELMINA KOMMUN
VUALTJEREN TJÏELTE

Inledning

Informationssäkerhetspolicy för Vilhelmina kommun

Vilhelmina kommuns informationssäkerhetspolicy fastställs av kommunfullmäktige och uttrycker ledningens övergripande inriktning och krav för informationssäkerhetsarbetet inom kommunen. Policyn utgör grunden för allt arbete med informationssäkerhet och kompletteras av särskilda riktlinjer som reglerar det praktiska genomförandet.

Syftet med policyn är att tydliggöra kommunens förhållningssätt till informationssäkerhet och säkerställa att all information – oavsett om den är muntlig, pappersburen eller digital – vid varje given tidpunkt har ett ändamålsenligt skydd.

Informationssäkerhetsarbetet ska vara dynamiskt och kontinuerligt anpassas efter aktuella hotbilder, både interna och externa. Det kan exempelvis handla om bristande kunskap hos medarbetare, fysiska intrång, leveranskedjestörningar eller cyberangrepp mot kommunens IT-miljö.

Denna policy omfattar hela kommunkoncernen.

Vad är informationssäkerhet?

Informationssäkerhet handlar om att skydda kommunens informationstillgångar genom ändamålsenliga säkerhetsåtgärder. Målet är att säkerställa att informationen hanteras på ett sätt som bevarar dess:

- **Konfidentialitet** – att information inte görs tillgänglig eller avslöjas för obehöriga.
- **Riktighet** – att informationen är korrekt, aktuell och fullständig.
- **Tillgänglighet** – att informationen är åtkomlig och användbar för behöriga när den behövs.

Informationssäkerheten ska alltid anpassas efter verksamhetens behov och riskbild, så att skyddet är **ändamålsenligt och proportionerligt** – varken överdrivet eller otillräckligt – i förhållande till informationens värde och känslighet.

För att kunna arbeta systematiskt och effektivt med informationssäkerhet är det viktigt att förstå ett antal centrala begrepp. Dessa definieras i de tillhörande riktlinjerna för informationssäkerhet.

Varför arbetar vi med informationssäkerhet?

Informationssäkerhet är en förutsättning för att Vilhelmina kommun ska kunna bedriva sin verksamhet på ett tryggt, lagligt och effektivt sätt. I takt med samhällets digitalisering ökar både beroendet av information och risken för att den utsätts för olika typer av hot. Cyberangrepp, desinformation, sabotage, otillbörlig åtkomst och oavsiktliga misstag är exempel på händelser som kan få allvarliga konsekvenser för kommunens verksamhet, invånarnas förtroende och individers integritet.

Omvärldsläget präglas av en ökad hotbild mot offentlig sektor, där kommuner är särskilt utsatta mål för både organiserad brottslighet och antagonistiska statliga aktörer. Samtidigt skärps kraven från nationella och internationella regelverk, såsom:

- NIS2-direktivet – som ställer krav på säkerhet i nätverk och informationssystem.
- CER-direktivet – som ställer krav på kontinuitet och verksamhetsskydd i samhällskritiska verksamheter.
- Dataskyddsförordningen (GDPR) – som kräver att personuppgifter hanteras med hög säkerhet och respekt för individens rättigheter.
- Offentlighetsprincipen och arkivlagen – som ställer krav på korrekt och tillgänglig informationshantering.
- Säkerhetsskyddslagen – som reglerar skyddet av säkerhetskänslig verksamhet.

För att möta dessa krav och skydda kommunens informationstillgångar krävs ett systematiskt, riskbaserat och långsiktigt informationssäkerhetsarbete. Det handlar inte bara om teknik, utan också om medvetenhet, rutiner och ansvarstagande i hela organisationen.

Genom att arbeta aktivt med informationssäkerhet stärker vi kommunens motståndskraft, skyddar våra invånare och säkerställer att vi kan leverera samhällsviktiga tjänster även under störningar.

Styrdokumentstruktur och relation till andra styrdokument

Ledningssystem för informationssäkerhet (LIS) – Styrdokumentstruktur

För att säkerställa ett systematiskt och enhetligt arbete med informationssäkerhet i Vilhelmina kommun finns riktlinjer som konkretiserar bestämmelserna i denna policy. Policy och tillhörande riktlinjer och rutiner utgör kommunens ledningssystem för informationssäkerhet.

För att möjliggöra en aktiv anpassning av verksamheten till omvärldsutvecklingen och rådande hotbild, beslutas informationssäkerhetspolicyn av kommunfullmäktige och informationssäkerhetsriktlinjerna beslutas av kommunchef.

Denna ansvarsfördelning gör att den övergripande strategin och åtagandena förankras politiskt, samtidigt som riktlinjerna – som styr det operativa informationssäkerhetsarbetet i detalj – anpassas kontinuerligt utifrån aktuella behov och förutsättningar.

Relation till andra styrdokument

Denna informationssäkerhetspolicy utgör det övergripande styrdokumentet för organisationens informationssäkerhet och kompletteras av andra relaterade policyer, riktlinjer och instruktioner.

Policyn ska läsas tillsammans med organisationens övriga styrdokument som berör informationssäkerhet. Dokumenten stödjer varandra och ska tillsammans skapa en helhetsbild av organisationens informationssäkerhetsarbete.

Vid eventuella konflikter eller tolkningsfrågor mellan olika styrdokument gäller denna informationssäkerhetspolicy som det överordnade dokumentet inom informationssäkerhetsområdet.

Informationssäkerhetsmål

Vilhelmina kommuns mål med informationssäkerhetsarbetet är att:

- Informationssäkerheten ska vara ett stöd i att förverkliga kommunens vision och strategiska inriktning.
- En ändamålsenlig och tydlig organisation för informationssäkerhet ska etableras och implementeras.
- Arbetet med informationssäkerhet ska ske strukturerat, riskbaserat och med långsiktighet.
- En kultur präglad av säkerhetsmedvetenhet, ansvarstagande och öppenhet ska främjas och prioriteras.
- Kritiska informationstillgångar ska identifieras, klassificeras och skyddas utifrån behov.
- Kommunens hantering av information ska präglas av transparens och skapa förtroende hos medborgarna.

Kommunens åtagande

Kommunens ställningstagande inom informationssäkerhet innebär att verksamheten ska:

- Bedriva informationssäkerhetsarbetet systematiskt och långsiktigt genom ett ledningssystem med utgångspunkt av ISO/IEC 27001[1], och med vägledning från ISO/IEC 27002. Ledningssystemet ska möjliggöra styrning, uppföljning och kontinuerlig förbättring.
- Säkerhetsåtgärder som vidtas ska utgå från Bilaga A i ISO/IEC 27001 och anpassas efter kommunens riskbild och behov.
- Uppfylla gällande lagkrav som reglerar kommunens informationssäkerhetsarbete.

Styrande principer

Kommunens ställningstagande inom informationssäkerhet innebär att verksamheten ska utgå från följande principer:

1. **Engagemang**
   Informationssäkerhetsarbetet ska präglas av ett aktivt engagemang från ledning, verksamheter och medarbetare. Alla nivåer inom organisationen har ett gemensamt ansvar för att främja en trygg, säker och ansvarsfull informationsförvaltning.
2. **Systematik**
   Arbetet med informationssäkerhet ska vara strukturerat och metodiskt. Det ska utgå från vedertagna ramverk såsom ISO/IEC 27001 och 27002, och integreras i kommunens ordinarie styrning och verksamhetsplanering.
3. **Kontinuerlig förbättring**
   Informationssäkerhetsarbetet ska vara iterativt, lärande och anpassningsbart. Erfarenheter, händelser och förändrade behov ska systematiskt leda till förbättring av rutiner, skyddsåtgärder och säkerhetsmedvetandet i organisationen.

[1] ISO/IEC 27001 är en internationell standard för ledningssystem för informationssäkerhet, som fastställer krav för att systematiskt skydda information. ISO/IEC 27002 kompletterar denna genom att ge praktisk vägledning för val och tillämpning av säkerhetsåtgärder. ISO/IEC 27000-serien omfattar ett antal relaterade standarder som tillsammans stödjer ett heltäckande arbete med informationssäkerhet, inklusive riskhantering, personalsäkerhet och kontinuitetsplanering.

VILHELMINA KOMMUN
VUALTJEREN TJÏELTE

Informationssäkerhetsorganisation

För att informationssäkerheten ska skapa engagemang i alla led, bedrivas systematiskt och bidra till kontinuerlig förbättring, behövs en tydlig organisation med fastställda roller, ansvar och fungerande samverkansformer. En sådan struktur stärker styrningen, klargör ansvarsfördelningen och skapar goda förutsättningar för ett systematiskt informationssäkerhetsarbete som uppfyller både lagkrav och främjar en god förvaltningskultur.

Kommunfullmäktige

Fastställer den övergripande policyn och målen för informationssäkerhet. Säkerställer att kommunstyrelsen förvaltar det politiska ansvaret för kommunens informationssäkerhetsarbete i enlighet med lagkraven och det fastställda ledningssystemet för informationssäkerhet.

Kommunstyrelsen

Bär det yttersta ansvaret för kommunens informationssäkerhet. Övervakar att denna policy efterlevs genom regelbundna rapporter från kommunchef.[2] Säkerställer att kommunala bolag, stiftelser, förbund och andra kommunala juridiska personer följer lagkraven och det fastställda ledningssystemet för informationssäkerhet.

Kommunchef

Bär det yttersta operativa ansvaret för hela kommunens informationssäkerhetsarbete. Fastställer riktlinjer, allokerar resurser och ansvarar för att organisationen följer beslutad policy.

Ledningsgrupp

Kommunchef tillsammans med verksamhets- och enhetschefer säkerställer att ledningssystem för informationssäkerhet implementeras i hela organisationen och prioriterar resurser för säkerhetsåtgärder.

Processledare för informationssäkerhet (CISO)

Ansvarar för att leda, inrikta, samordna och utvärdera kommunens informationssäkerhetsarbete. Återrapporterar till kommunstyrelsens ordförande och kommunchef.

IT-säkerhetsstrateg

Ansvarar för att kravställa, samordna och inrikta IT-säkerhetsarbetet på både övergripande och verksamhetsnivå. Säkerställer att tekniska säkerhetsåtgärder implementeras enligt organisationens behov och riktlinjer. Samverkar med IT-enheten och återrapporterar till kommunchef.

---

[2] Enligt *Lagrådsremiss: Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* (2025) omfattar cybersäkerhetslagen inte kommunfullmäktige.

GDPR-samordnare

Samordnar kommunens dataskyddsarbete enligt GDPR. Stödjer verksamheterna i dataskyddsfrågor och säkerställer regelefterlevnad.

Dataskyddsombud (DSO)

Oberoende kontrollfunktion som övervakar dataskyddsefterlevnad. Rådgör organisationen och är kontaktpunkt mot Integritetsskyddsmyndigheten (IMY).

Processansvarig

Den verksamhet eller funktion som ansvarar för en utpekad process inom organisationens informationssäkerhet ansvarar för att planera, utforma och följa upp processen i enlighet med fastställda krav. Vilka verksamheter som är processansvariga och för vilka processer framgår i Bilaga A.

Säkerhetskyddsorganisationen

Säkerhetsskyddsorganisationen ansvarar för att kommunens hantering av säkerhetsskyddsklassificerade uppgifter och säkerhetskänslig verksamhet uppfyller kraven i säkerhetsskyddslagstiftningen. Inom dessa områden gäller säkerhetsskyddslagen med företräde framför annan reglering.

Verksamhets- och enhetschefer

Ansvarar för att upprätthålla informationssäkerheten inom sitt specifika förvaltningsområde. Se Bilaga A för mer information.

Resursägare

Verksamhetsansvarig eller utses av kommunchef beroende på resurstyp. Ansvarar för att informationstillgångar, system, avtal och objekt identifieras, inventeras, klassas och skyddas. Se Bilaga A för mer information.

Resursförvaltare

Utses av resursägare. Stödjer resursägaren i att efterleva gällande riktlinjer och resursförvaltningsplaner. Hanterar tekniska systemändringar, uppdaterar dokumentation samt säkerställer att säkerhetskonfigurationer följs och underhålls.

Medarbetare

Alla anställda i kommunen. Följer informationssäkerhetsriktlinjer i det dagliga arbetet, deltar i obligatoriska utbildningar och rapporterar incidenter omgående.

Informationssäkerhetsråd

Ett rådgivande forum som samlar processledare för informationssäkerhet (CISO), IT-säkerhetsstrateg, GDPR-samordnare, processansvariga och verksamhets representanter för att diskutera, samordna och följa upp frågor kopplade till den verksamhetsnära informationssäkerheten. Rådet stödjer informationssäkerhetsarbetet genom att ge rekommendationer, identifiera behov och främja samsyn inom organisationen.

Informationssäkerhetsstyrgrupp

Ett styrande organ med uppdrag att inrikta, prioritera och följa upp det strategiska informationssäkerhetsarbetet inom organisationen. Gruppen säkerställer att informationssäkerheten är integrerad i verksamhetens övergripande styrning.

Avstegshantering

Om en verksamhet behöver göra avsteg från denna policy eller dess riktlinjer ska en inledande bedömning ske i samråd med kommunens processledare för informationssäkerhet (CISO).

Om CISO bedömer att avsteget kan vara motiverat, ska detta dokumenteras i en tjänsteskrivelse som lämnas in till kommunchefen för beslut om att tillstyrka eller avslå avstegen.

Vid godkännande gäller följande:

- Avsteget ska vara tidsbegränsat och omprövas senast efter två år.
- Om avsteget avser en resurs (till exempel informationssystem, avtal eller objekt) ska en riskbedömning och åtgärdsplan bifogas.
- Samtliga avsteg ska dokumenteras och följas upp inom det systematiska informationssäkerhetsarbetet.

Vid avslag ska verksamheten antingen justera sin begäran eller anpassa verksamheten för att följa gällande policy och dess riktlinjer. Verksamheten äger ansvaret under hela denna process.

VILHELMINA KOMMUN
VUALTJEREN TJÏELTE

Verksamhetskontroll och överträdelsehantering

CISO och IT-säkerhetsstrateg ansvarar för att regelbundet granska och följa upp hur organisationen arbetar med att utveckla och förbättra informationssäkerheten. Arbetet ska stödja en lärande säkerhetskultur och ett systematiskt förbättringsarbete.

Vid allvarliga överträdelser av lagkrav, policy, riktlinjer eller interna rutiner ska en dokumenterad process med fokus på organisatoriskt lärande tillämpas. Syftet är att säkerställa en transparent, konsekvent och konstruktiv hantering.

Följande principer ska vägleda processen:

Lärande – Orsaker ska analyseras för att möjliggöra kunskapsöverföring och förbättrade arbetssätt.

Ständig förbättring – Brister ska leda till konkreta åtgärder som stärker säkerheten.

Uppsåt – Skillnad ska göras mellan avsiktliga överträdelser och oavsiktliga misstag.

Aktsamhet – Bedömningen ska ta hänsyn till om individen/verksamheten agerat med rimlig försiktighet.

Resurser – Organisationens ansvar för att ha gett tillräckligt stöd och utbildning ska vägas in.

Vid behov vidtas åtgärder enligt gällande lagstiftning, interna regelverk och arbetsrättsliga principer. Allvarliga incidenter ska rapporteras till relevant ledningsnivå och, där det krävs, till relevant tillsynsmyndighet.

VILHELMINA KOMMUN
VUALTJEREN TJÏELTE

Bilaga A: Fördjupning av informationssäkerhetsorganisationen

Beredskapsfunktionen

Processansvarig för att krav på informationssäkerhet beaktas inom arbetet med civil beredskap, särskilt vid planering, utformning och uppföljning av kontinuitetshantering och krisledning.

IT-chef

Processansvarig för att det finns en fungerande, uppdaterad och dokumenterad process för tekniskt skydd (till exempel brandväggar, kryptering, behörighetsstyrning). Planerar, utformar och följer upp processen i samverkan med processledare för informationssäkerhet (CISO) och IT-säkerhetsstrateg.

Ekonomichef

Processansvarig för att det finns en process för säker hantering av leverantörer och leveranskedjor (till exempel kravställning i upphandling, säkerhetsbilagor, uppföljning). Planerar, utformar och följer upp processen i samverkan med CISO och IT-säkerhetsstrateg.

Personalchef

Processansvarig för att det finns processer för personalsäkerhet (till exempel säker rekrytering, personalkännedom, introduktion, åtkomsthantering vid anställningsförändring och avslut). Planerar, utformar och följer upp processen i samverkan med CISO och IT-säkerhetsstrateg.

Kanslichef

Processansvarig för att planera, utveckla och följa upp kommunövergripande processer för informationsförvaltning (till exempel dokumentmallar, diarieföring, informationshanteringsplan), i samverkan med CISO och IT-säkerhetsstrateg.

Verksamhets- och enhetschefer

Ansvarar för att upprätthålla informationssäkerheten inom sitt specifika förvaltningsområde. Det innebär att implementera gällande riktlinjer, ta fram verksamhetsspecifika rutiner samt utöva resursägarskap och ansvara för resursförvaltning. I ansvaret ingår även kontinuitetshantering, resurssäkerhet och att säkerställa personalsäkerheten. Verksamheterna ska dessutom se till att personalen får tillräcklig utbildning i informationssäkerhet och att eventuella incidenter rapporteras vidare inom organisationen.

Resursägare

Upprättar en förvaltningsplan för varje enskild resurs, som årligen ska utvärderas och revideras. Resursägaren ansvarar även för att det finns en samlad inventarielista över samtliga informationstyper och mängder, IT- och OT-system, avtal och objekt som uppdateras årligen. Inventarielistan ska ligga till grund för klassificering, riskanalys och prioritering av skyddsåtgärder.