Stödanvisning säker kommunikation och lagring

Östhammars kommun

Målgrupp	Chefer och nyckelpersoner, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-12-09
Reviderad	2026-03-05

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

Innehåll

Innehållet i stödanvisningen utgår från Östhammar kommuns (kommunens) program och vägledning för informationssäkerhet. Den ger exempel och riktlinjer för hur information klassad på olika nivåer kan hanteras, kommuniceras och lagras på ett säkert sätt inom kommunens verksamheter. I stödanvisningen förutsätts att de verktyg, system och tjänster som kommunen tillhandahåller och förvaltar används.

Mål och syfte

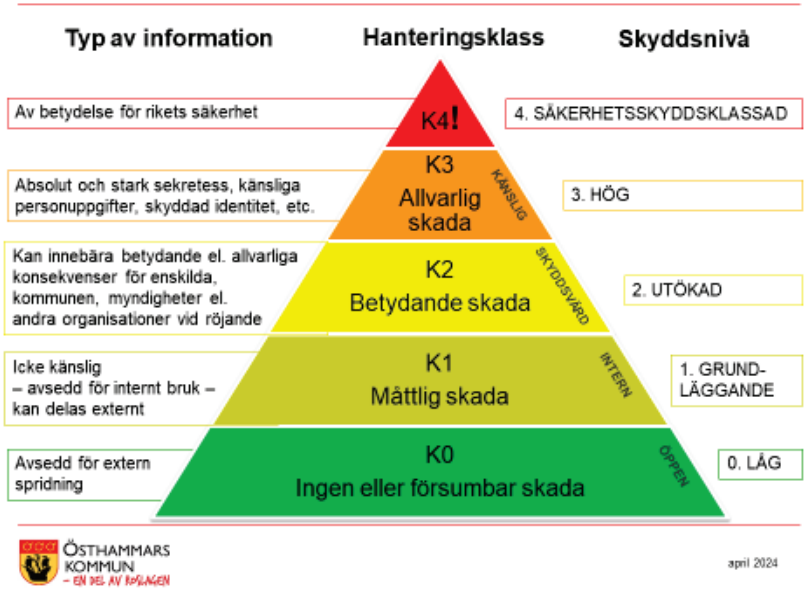
Målet är att underlätta för medarbetare och chefer som hanterar skyddsvärd och känslig information. Syftet är att minska risken för att uppgifter hanteras på ett felaktigt sätt, nås av obehöriga och därigenom kan missbrukas, manipuleras och förstöras.

Öppen, intern, skyddsvärd och känslig information

Den information kommunen hanterar är i grunden öppen. Kommunen ska vara transparant och i det ingår en skyldighet att lämna ut information och handlingar när allmänheten, massmedia eller andra efterfrågar dem. Handlingsoffentligheten är ett uttryck för offentlighetsprincipen, vilken regleras i tryckfrihetsförordningen. Tanken är att insyn och öppenhet ska öka rättssäkerheten och effektiviteten i myndigheternas arbete, förhindra rättsövergrepp mot enskilda, motverka korruption och stärka allmänhetens förtroende.

Det finns också bestämmelser om sekretess i offentlighets- och sekretesslagen som begränsar rätten att ta del av allmänna handlingar. Vidare har kommunen har en skyldighet att se till att skyddsvärd och känslig information hanteras på ett säkert sätt och ges ett ändamålsenligt skydd genom hela sin livscykel och oavsett var den kommuniceras och lagras. Verksamheternas informationsklassning ger underlag för beslut om hur informationen ska hanteras och skyddas. Triangeln nedan illustrerar olika informationstyper, hanteringsklasser och skyddsnivåer. Med varje skyddsnivå följer olika säkerhetskrav och skyddsåtgärder. K står för konfidentialitet.

Hantering av information klassad i olika konfidentialitetsnivåer



Konfidentialitet nivå 0 (K0) – ingen eller försumbar skada – låg skyddsnivå
Den information som en informationsägare klassar på K0-nivå är avsedd för extern spridning och kan kommuniceras i de kanaler som verksamheten normalt använder för extern kommunikation. Den kan även kommuniceras internt. Detsamma gäller lagring. Informationen behöver *inte* något specifikt skydd utöver det som redan finns i de tjänster, kanaler och lagringsplatser som kommunen förvaltar, tillhandahåller och använder. Om informationen sprids bredare har bedömningen gjorts att det *inte* ger några skadeverkningar alls eller att skadan är försumbar.

Konfidentialitet nivå 1 (K1) – måttlig skada - grundläggande skyddsnivå
Den information som en informationsägare klassar på K1-nivå är avsedd för en intern målgrupp och kan kommuniceras i de kanaler som verksamheten normalt använder för intern kommunikation. Detsamma gäller lagring. Att information är K1-klassad innebär att den *inte* är av känslig karaktär och endast behöver ett grundläggande skydd – det skydd som redan finns i de kanaler och på de lagringsplatser som kommunen tillhandahåller, förvaltar och använder. Om K1-information skulle spridas till fler interna målgrupper eller externt bedöms skadan som måttlig.

Konfidentialitet nivå 2 (K2) – betydande skada – utökad skyddsnivå
Den information som en informationsägare klassar på K2-nivå är avsedd för en begränsad intern och/eller extern målgrupp. Informationen ska hanteras på ett säkert sätt genom hela sin livscykel och får endast behandlas, kommuniceras och lagras i de kanaler, system och tjänster som är klassade för att kunna hantera skyddsvärd information. K2-klassad information kräver ett utökat skydd och att tillgången till informationen begränsas till de personer eller grupper som är behöriga att ta del av den. Om skyddsvärda uppgifter skulle spridas till obehöriga skulle det kunna innebära betydande negativ påverkan för exempelvis enskilda personer, kommunen och/eller andra aktörer i samhället.

Konfidentialitet nivå 3 (K3) – allvarlig skada – hög skyddsnivå
Den information som en informationsägare klassar på K3-nivå är avsedd för en mycket begränsad intern och/eller extern målgrupp. Känsliga och sekretessbelagda uppgifter klassificerad på K3-nivå har ett högt skyddsvärde och det är viktigt att informationen hanteras på ett säkert sätt genom hela sin livscykel. Det innebär att denna information endast får lagras, delas och skickas krypterad via säkra kanaler och att endast de behöriga personer som verkligen behöver informationen ska ha möjlighet att få tillgång till den.

Konfidentialitet nivå 4 (K4) – synnerligen allvarlig skada - säkerhetsskyddsklassad
Information av betydelse för Sveriges säkerhet och som kan påverka landets totalförsvarsförmåga om uppgifterna röjs. Dessa uppgifter ska endast hanteras av Säkerhetsskyddschef enligt kommunens rutin för hemlig information och säkerhetsskyddslagen. Vid osäkerhet om information ska säkerhetsskyddsklassas kontakta i första hand säkerhetsskyddschef, i andra hand informationssäkerhetssamordnare.

Exempel på information klassad på olika konfidentialitetsnivåer

Informationsklass/Exempel	K0	K1	K2	K3	Kommentarer
Aggregerad information om klassning, risker, sårbarheter och prioriteringar				X	På papper eller i system
Anbud upphandling - pågående – absolut sekretess				X	
Annonser, t.ex. rekryteringsannonser	X				
Arkivet				X	
Avtal		X			
Bygglov		X			
Bygglov från Vattenfall (Forsmark)			X		
Ansökningar, t.ex. jobbansökningar		X			
Kartskikt, ritningar och uppgifter som beskriver kritisk infrastruktur, känsliga anläggningar, skyddsvärda objekt, etc.				X	Mycket känsliga uppgifter som ska hanteras enligt särskild rutin
Kontinuitetsplaner och **beredskapsplaner**			X	X	Kan innehålla mycket känsliga uppgifter, men behöver inte göra det. I en aggregerad form, dvs. om de samlas på ett ställe bedöms de vara på K3-nivå.
Koder				X	
Löneuppgifter (offentlig handling)		X			
Lösenord				X	
Nyckelbefattningar			X		
Nyheter på osthammar.se	**X**				
Informationssäkerhetsincidenter – rapporter				X	
IT servicefönster (inloggat läge på Ines)		X			
IT - information om störningar, problem och incidenter				X	
Personuppgifter, vanliga, enstaka, t.ex. namn och mejl-adress utan koppling till skyddsvärda eller känsliga uppgifter		X			
Personuppgifter, skyddsvärda, t.ex. listor med många namn, adresser, etc. samt personuppgifter kopplade till fler uppgifter om individer eller grupper			X		

Personuppgifter, känsliga[1], t.ex. utredningar om barn, elevdata- och omdömen, uppgifter om brukare, personliga förhållanden, hälsa, allergier, vård, omsorg, journaler, religiös och politisk åskådning, etc.				X	Känsliga personuppgifter ska hanteras enligt särskild rutin.
Personuppgifter, skyddade[2],				X	Skyddade personuppgifter är mycket känsliga uppgifter som behöver hanteras enligt särskild rutin.
Referenstagning vid rekrytering			X		
Reservkraft skyddsvärda anläggningar				X	Mycket känsliga uppgifter som ska hanteras enligt särskild rutin
Risk- och sårbarhetsanalyser (RSO)	X			X	RSA kan delas upp i en öppen K0-del och en känslig K3-del med olika skyddsåtgärder.
Servrar – kritisk infrastruktur				**X**	

Hanteringsklass och märkning

All information ska märkas med konfidentialitetsnivå och hanteringsklass för att säkerställa att både sändare och mottagare av informationen vet hur den ska hanteras genom hela sin livscykel. Ett tekniskt stöd för detta kommer att möjliggöras i takt med att kommunen inför Microsoft 365.

- K0-klassad information märks med **K0, ÖPPEN** (Grön vid färgmarkering)
- K1-klassad information märks med **K1, INTERN** (Mossgrön vid färgmarkering)
- K2-klassad information märks med **K2, SKYDDSVÄRD** (Gul vid färgmarkering)
- K3-klassad information märks med **K3, KÄNSLIG** (Orange vid färgmarkering)
- K4-klassad information - märks och hanteras enligt rutin för hemlig information

[1] Läs mer om personuppgifter hos IMY: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/
[2] Sekretessmarkering - en varningssignal för myndigheter. Markeringen syns i folkbokföringsregistret men uppgifterna får inte lämnas ut utan tillstånd och säkerhetskontroll. Skyddad folkbokföring - ett förstärkt skydd - en person kan vara folkbokförd i en kommun och bo i en annan. Kommunen kan se att en person har skyddad folkbokföring. Fingerade personuppgifter - en person får nya identitetsuppgifter, t.ex. nytt namn och personnummer. Personens gamla identitet tas bort ur folkbokföringsregistret.

Notera att externa organisationer ansvarar för att klassa och märka sin information, men de kan använda en annan terminologi och märkning. I de fall det är otydligt vad som gäller för säker informationshantering, dubbelkolla med avsändaren.

Säkra tekniska lösningar för kommunikation och lagring

Kommunen tillhandahåller och använder krypteringslösningar och säkra kommunikations- och lagringstjänster som t.ex. säker e-post och säkra digitala möten. Dessa ska användas för säker kommunikation då fysiska möten inte är ett alternativ. För att utbyta känslig och sekretessbelagd information mellan kommuner, regioner och statliga myndigheter ska säker digital kommunikation (SDK) användas med start 2025.

Krav på system, tjänster och leverantörer vid hantering av skyddsvärd och känslig information

Det ska vara verifierat och dokumenterat att de system, tjänster, e-tjänster, integrationer, etc. som hanterar information som verksamheterna klassat på K2- och K3-nivå klarar informationssäkerhetskraven och har ett ändamålsenligt skydd. Tekniska lösningar, verktyg och mallar ska också möjliggöra en synlig märkning som visar informationens klassning och hanteringsregler (öppen, intern, skyddsvärd, känslig).
Leverantörer som kan få tillgång till eller som ska använda, behandla eller hantera känslig och skyddsvärd information ska skriva under kommunens sekretessavtal. I de fall det gäller personuppgifter ska det alltid finnas PUB-avtal mellan kommunen och organisationen.

Hanteringsregler

Nedan specificeras hanteringsregler för information klassad på olika konfidentialitetsnivåer.

- Grönt: JA
- Rött: NEJ

Informationsklass/ Säker informations-hantering	Vanlig e-post	Vanlig e-post + krypterad fil[3]	Säker e-post[4]	Vanliga videomöten t.ex. Teams	Säkra videomöten, t.ex. Skiffer	System/tjänster godkända för K0-K1-info	System/tjänster godkända för K2-K3- info	Filserver, projektplats, Teams, etc.	Filserver behörighets-styrd	Säker Filyta behörighetsstyrd, + MFA[5]	Office 365 lagring (Onedrive)
K0	JA	JA	JA	JA	JA	JA	JA	JA	JA	JA	JA
K1	JA	JA	JA	JA	JA	JA	JA	JA	JA	JA	JA
K2	NEJ	JA	JA	NEJ	JA	NEJ	JA	NEJ	JA	JA	NEJ
K3	NEJ	NEJ	JA	NEJ	JA	NEJ	JA	NEJ	NEJ	JA	NEJ
K4[6]	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ

Vägledning, stöd och kontakt

Stödmaterial nås via Ines Vägledning och stöd.

Vid frågor, kontakta:

- Informationssäkerhetsteamet via funktionsbrevlådan infosakerhet@osthammar.se (bevakas vardagar) alternativt via Teams eller telefon; Maria Langen (informationssäkerhetssamordnare) 0173-861 08, Håkan Åhlénius (dataskyddsamordnare) 0173-854 12 och Anneli Lennström (Informationssäkerhetsteamet) 0173-862 43
- Beredskapsteamet via funktionsbrevlådan beredskap@osthammar.se (bevakas vardagar) alternativt via Teams eller telefon; Säkerhetsskyddchef Elin Fogelström 0173-860 32

[3] Obs! Krypteringsnyckel eller kod måste delas på annat sätt än i e-postmeddelandet
[4] Säker e-post är en krypterad tjänst för att skicka meddelanden mellan individer. Säker digital kommunikation (SDK) används för att skicka känslig information mellan myndigheter, regioner och kommuner.
5 Multifaktorautentisering (MFA) ger ytterligare ett skyddslager i inloggningsprocessen. Vid åtkomst till konton eller appar genomgår användarna ytterligare en identitetsverifiering, till exempel med fingeravtrycksavläsning eller en kod som skickas till telefonen.
[6] K4-information hanteras enligt rutin för hemlig information. Kontakta säkerhetsskyddchef eller informationssäkerhetssamordnare vid gränslandsfrågor.