# Informationssäkerhet

## Stödanvisning
## klassificering av information

## Östhammars kommun

| | |
|---|---|
| Målgrupp | Chefer och nyckelpersoner, alla kontor och verksamheter |
| Avsändare | Kommunledningskontoret, Digitalisering och projektledning |
| Dokumentansvarig | Informationssäkerhetssamordnare |
| Framtagen | 2024-10-10 |
| Aktualitetsprövad | 2026-03-05 |

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

# Innehåll

## Innehåll

Innehållet utgår från kommunens program och vägledning för informationssäkerhet och ger en fördjupad beskrivning och förklarar arbetsprocessen med att ***klassificera*** den information, inklusive personuppgifter, som kommunens verksamheter hanterar.

## Mål och syfte

Målet är en ensad process för klassning som svarar mot externa krav, interna behov och som bidrar till att skydda informationen i kommunens verksamheter.
Syftet är att säkra kvalitén i kommunens arbete med informationssäkerhet genom att klassa informationen och identifiera omständigheter som kräver kontroll, åtgärd och uppföljning. Arbetet omfattar även de IT-tjänster som används för kommunens informationshantering.

# Klassning

Klassningen utgör underlag för hur informationen ska hanteras, behandlas och skyddas.
En informationsklassnings hållbarhet är kortvarig då information fortlöpande förändras och det kan tillkomma ny information av känslig karaktär. Även organisationsförändringar, ny teknik och integrationer kan ge förändrade förutsättningar. Informationsklassningen ska därför följas upp årligen - eller oftare vid behov. Om det är samma information och hantering som tidigare påverkar det inte klassningen, man noterar då ”Ingen förändring” och datum. Om det har skett en förändring och den är betydande måste klassningen göras om.

## Dokumentation

Informationsklassningar ska dokumenteras och aktuella versioner finnas tillgängliga i respektive verksamhet. I kommunens verktyg Security dokumenterar informationssäkerhetsteamet aktuella informationstillgångar (som t.ex. system och applikationer) med en beskrivning av den information som hanteras, tillgångarnas påverkan, legala krav, beroende m.m. Om inte klassningen är gjord tillsammans med informationssäkerhetsteamet - och därmed redan dokumenterad i verktyget Security - är det viktigt att komma ihåg att skicka en kopia på klassningen till infosakerhet@osthammar.se.
Om klassningen innehåller känsliga uppgifter, kolla med informationssäkerhetsteamet vilken säker kanal som kan användas.
För personuppgifter gäller att de även ska vara dokumenterade i en registerförteckning enligt kraven i dataskyddsförordning – dokumenteras i kommunens verktyg Integrity av utsedda kontaktpersoner.

## Klassning steg för steg

**Steg 1**
**Bestäm informationens skyddsvärde utifrån nedanstående:**

- Vilken funktion och betydelse har den för verksamheten?
- Vilka konsekvenser medför det för verksamheten om informationen förändras av obehörig, försvinner, kommer i orätta händer eller inte går att nå?
- Hur känslig är informationen för den enskildes personliga integritet?

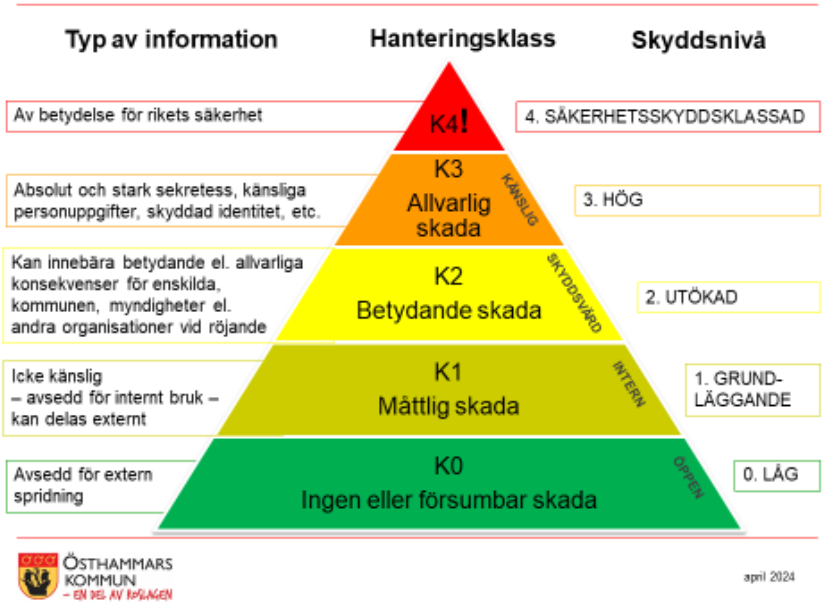
*Bedömningen görs oberoende av om det är ett IT-system, en webbtjänst eller ett papper som bär informationen.*

Informationens skyddsvärde fastställs utifrån skalan 0-3 och utgår från aspekterna KRT.
**Konfidentialitet (K)** – vilka konsekvenser medför det om någon obehörig kommer åt informationen?
**Riktighet (R) –** vilka konsekvenser medför det om någon obehörig har ändrat informationen så den inte är tillförlitlig?
**Tillgänglighet (T)-** vilka konsekvenser medför det om informationen inte går att nå inom önskad tid?

Nivå 0 (Ingen eller försumbar skada), Nivå 1 (Måttlig skada), Nivå 2 (Betydande skada), Nivå 3 (Allvarlig skada)

Ju större konsekvensen bedöms kunna bli för verksamheten om informationen inte skyddas, desto högre skyddsvärde ska anges för informationen.
Alla bedömningar ska dokumenteras (motivera/förklara skyddsvärdet) för att stödja det kollektiva minnet, undvika personberoende och underlätta uppföljningsarbete.

Triangeln illustrerar olika informationstyper, hanteringsklasser och skyddsnivåer. K står för konfidentialitet. Med varje skyddsnivå följer olika säkerhetskrav och skyddsåtgärder.




**Steg 2**
**Ta ställning till skyddsåtgärder/säkerhetsåtgärder**
När informationens värde är fastställt (steg 1) är det dags att ta ställning till skyddsåtgärder. *Skyddsåtgärder* är en del av säkerhetsåtgärder och är specifikt inriktade på att minska sannolikheten för att en säkerhetsincident inträffar genom att direkt skydda mot hot och minska sårbarheter. *Säkerhetsåtgärder* är bredare och omfattar alla åtgärder för att hantera informationssäkerhetsrisker och skydda informationstillgångar.

Säkerhetsåtgärderna delas in i fyra huvudsakliga kategorier, enligt ISO-standard 27002:

- *Organisatoriska säkerhetsåtgärder*: Dessa handlar om processer och rutiner för att hantera informationssäkerhet på ett strukturerat sätt, t.ex. riskhantering, handlings- och kontinuitetsplaner samt utbildningsinsatser är andra exempel.
- *Personrelaterade säkerhetsåtgärder:* dessa omfattar åtgärder kopplade till anställda och andra personer som har tillgång till information, t.ex. säkerhetsutbildning, bakgrundskontroller och tydliga ansvarsområden.
- *Fysiska säkerhetsåtgärder:* dessa åtgärder skyddar den fysiska miljön där information hanteras, t.ex. låssystem, övervakningskameror och kontrollerad tillgång till byggnader.
- *Tekniska säkerhetsåtgärder***:** dessa innefattar tekniska lösningar för att skydda information och system, t.ex. brandväggar, antivirus, kryptering och åtkomstkontroller.

Dessa åtgärder ska ses som en lägstanivå där kompletteringar och anpassningar kan göras vid behov. Ta stöd av informationssäkerhetsteamet om osäkerhet finns kring vilka säkerhetsåtgärder som kan behövas utifrån klassning
En grundläggande princip är att ju större skyddsvärde informationen har desto mer omfattande åtgärder behövs för att skydda informationen.

**Börja med:**

1. **Ta ställning till** vilka verksamhetsnära skyddsåtgärder som redan finns på plats och vilka som behöver arbetas in av verksamheten.
   Informationsägaren ansvarar för att dessa krav kommuniceras till berörda ansvariga.
   Om det gäller ett system behöver systemägaren ta ställning till vilka tekniska skyddsåtgärder som redan finns på plats och vilka som behöver arbetas in.
   Informationsägaren ansvarar för att kommunicera de tekniska kraven till systemägaren som ansvarar för IT-tjänsten
2. **Bedöm** om skyddsåtgärderna behöver kompletteras med konsekvensbedömning[1] enligt dataskyddsförordningen med hjälp av dataskyddsamordnaren (informationssäkerhetsteamet)
3. **Kravställ**
   Skyddsåtgärderna ingår sedan som kravställning vid upphandling och utveckling av tjänster och produkter som hanterar kommunens information, se *Stödanvisning för anskaffning och utveckling.*

Efter genomgångna säkerhetsåtgärder är det dags att dokumentera och hantera risker, *se Stödanvisning för riskhantering.*

[1] En utredning som beskriver en personuppgiftsbehandling och dess syfte, bedömer behovet och eventuella risker i personuppgiftsbehandlingen m.m

# Mall för dokumentation

Mall för klassning av information nås via INES Klassa information och Vägledning och stöd