



**VARBERGS
KOMMUN**

Riktlinjer för informationssäkerhet

Dokumenttyp: Riktlinje	Dokumentnamn: Riktlinjer för informationssäkerhet	Diarienummer: KS 2019/0562
Beslutad av: Kommunstyrelsen	Beslutsdatum: 2019-12-17, § 287	Giltig till och med: Tillsvidare
Gäller för: Varbergs kommun	Dokumentansvarig avdelning: Kommunkansliet	Senast reviderad:

Riktlinjer för informationssäkerhet

Inledning

Varbergs kommuns policy för informationssäkerhet är ett övergripande dokument som redovisar kommunens mål och inriktning för arbetet med informationssäkerhet. Riktlinjer för informationssäkerhet konkretiserar policyn.

Riktlinjernas omfattning

Riktlinjerna innehåller en översiktlig information om hur en god informationssäkerhet ska uppnås vid all hantering av information inom Varbergs kommuns samtliga verksamheter.

Introduktion till informationssäkerhet

Informationssäkerhet består av att skapa och upprätthålla lämpligt skydd för information oavsett dess form så som text, bild, film och ljud oberoende av om den finns i IT-system, papper eller i form av tal. Medan IT-säkerhet fokuserar på säkerhet i IT-miljöer så handlar informationssäkerhet om hur all information ska skyddas oavsett hur den hanteras.

Informationssäkerhet utgörs av tre viktiga delar där informationen ska vara:

- konfidentiell - att endast behöriga personer får ta del av den
- riktig - att vi kan lita på att den är korrekt och inte manipulerad eller förstörd
- tillgänglig – att den alltid finns när vi behöver den

Rättsliga krav i form av lagar, förordningar, föreskrifter och avtal ställer ofta även krav på en verksamhets informationshantering vilket inbegriper krav på konfidentialitet, riktighet och tillgänglighet.

Olika typer av oönskade händelser (incidenter), vilka kan vara oavsiktliga eller avsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationen.

Ett systematiskt och proaktivt informationssäkerhetsarbete bidrar till att informationen uppfyller rättsliga krav och skyddas mot oönskade händelser.

Styrning och ansvar för informationssäkerheten

Kommunfullmäktige uttrycker sin viljeriktning genom Policy för informationssäkerhet.

Kommunstyrelsen beslutar om riktlinjer för hur informationssäkerhetsarbetet ska bedrivas i enlighet med policyn. Kommunstyrelsen har även ansvar för samordning och uppföljning av arbetet med informationssäkerhet.

Varje nämnd och styrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde och i förekommande fall även för tillhörande externa organisatoriska former om de saknar eget organisationsnummer.

Kommunstyrelse, nämnder och kommunala bolag är även personuppgiftsansvariga inom respektive verksamhetsområde. Som personuppgiftsansvarig har de det yttersta ansvaret för att all behandling av personuppgifter sker i enlighet med Dataskyddsförordningen.

Organisation för informationssäkerhetsarbetet

Kommunens övergripande informationssäkerhetsarbete samordnas av en informationssäkerhetsstrateg på kommunstyrelsens förvaltning.

Kommundirektören beslutar inom ramen för verkställighet om en övergripande anvisning, "Anvisning för informationssäkerhetsarbetet". Anvisningen beskriver hur arbetet organiseras för den kontinuerliga hanteringen av detaljerade instruktioner och vägledningar.

Kommunen har även ett utsett dataskyddsbud för alla nämnder och bolag vilket är ett krav enligt dataskyddsförordningen. Dataskyddsbudets oberoende roll är att kontrollera att dataskyddsförordningen, GDPR, följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

Kommunen har också olika arbetsgrupper för frågor som berör informationssäkerhet.

Informationsklassning

Informationsklassning är en grundläggande del i arbetet med systematisk informationssäkerhet. Genom att klassificera information utifrån aspekterna konfidentialitet, riktighet och tillgänglighet får vi förståelse för, och kan styra det skydd som krävs för olika informationsmängder.

Klassning av information ska ske utifrån rättsliga krav, men även interna krav på informationens värde och betydelse för verksamheterna ska vägas in.

Notera att informationsklassningen i detta dokument inte omfattar eller på något vis beskriver information som faller inom ramen för säkerhetsskyddslagen. Information av detta slag har betydligt högre skyddskrav.

Varbergs kommuns modell för informationsklassning

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
3. Höga skyddskrav	Konfidentiell information som, om den sprids till obehöriga, kan medföra allvarlig negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är riktig och fullständig, kan medföra allvarlig negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är tillgänglig, kan medföra allvarlig negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.
2. Förhöjda skyddskrav	Känslig information som, om den sprids till obehöriga, kan medföra betydande negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.
1. Normala skyddskrav	Harmlös information som, om den sprids till obehöriga, kan medföra måttlig negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan för Varbergs kommun, externa aktörer eller enskilda individer.
0. Låga skyddskrav	Öppen information kan i regel spridas fritt inom och utom Varbergs kommun.	Normala skyddskrav avseende informationens riktighet och tillgänglighet.	Normala skyddskrav avseende informationens riktighet och tillgänglighet.

Figur 1: Varbergs kommuns modell för informationsklassning

Beskrivning informationsklasser

- **Konfidentiell information** utgörs av uppgifter som berörs av sekretess eller av andra bärande skäl behöver hållas konfidentiell. Konfidentiell information får endast vara tillgänglig för enskilda medarbetare som har ett direkt behov av att hantera informationen
- **Känslig information** utgörs av sådana uppgifter som har ett något högre skyddsvärde än den som klassas som harmlös, men som samtidigt inte riktigt når upp till det skyddsbehov som finns för information som är klassad som konfidentiell. Vad som skiljer den från **harmlös information** är att det ställs högre krav på behörighet så att endast de medarbetare som har ett faktiskt och direkt behov av informationen får ha tillgång till den.
- **Harmlös information** kännetecknas av att den består av harmlösa personuppgifter så som namn, telefonnummer, adress, e-postadress, fastighetsbeteckning, användar-id med mera. Intern information av detta slag kan normalt vara tillgänglig för en avdelning, enhet eller arbetsgrupp som kan ha behov av att hantera informationen.
- **Öppen information** utgörs främst av all den information som inte består av några personuppgifter alls eller andra uppgifter som bedöms vara helt okänsliga för vidare spridning. Öppen information har normalt inga krav på åtkomstbegränsning utan kan normalt spridas fritt inom och utom Varbergs kommun.

Detaljerade instruktioner och vägledningar

Arbetet med informationssäkerhet i en kommun är mycket komplext och omfattande då det finns en mycket stor mängd information som hanteras i många olika system och på annat vis. Kommunens verksamheter styrs dessutom av en mängd lagar, författningar och förordningar vilka många gånger ställer direkta krav på hanteringen av information.

Varbergs modell för att hantera utmaningen är att under ordnade former hantera detaljerade instruktioner och vägledningar inom ramen för verkställighet.

Instruktioner sammanfaller med de övergripande riktlinjer som anges i detta styrdokument och de ska följas av kommunens verksamheter.

Vägledningar är främst rådgivande och bör följas av kommunens verksamheter.

Kontroll och uppföljning

Samtliga nämnder ska säkerställa lämpliga kontrollpunkter för informationssäkerheten.