



# Riktlinje för säkerhetskydd



## Innehållsförteckning- riktlinje för säkerhetsskydd

1. Inledning och syfte .....	3
2. Säkerhetsskyddsorganisation och ansvar .....	3
Kommunstyrelsen .....	3
Säkerhetsskyddschef.....	3
Kommundirektör, avdelningschefer, verksamhetschefer och VD för kommunala bolag. ....	3
3. Säkerhetsskyddsanalys och säkerhetsskyddsplan.....	4
Säkerhetsskyddsanalys .....	4
Säkerhetsskyddsplan.....	4
4. Informationssäkerhet .....	4
Administrativ säkerhet .....	4
IT-säkerhet.....	5
5. Fysisk säkerhet .....	5
6. Personalsäkerhet .....	5
7. Säkerhetsskyddad Upphandling (SUA) .....	6
8. Incidenthantering.....	6
9. Utbildning och uppföljning .....	6



## 1. Inledning och syfte

Säkerhetsskyddet i Valdemarsviks kommun är baserat på Säkerhetsskyddslagen (2018:585) och Säkerhetsskyddsförordningen (2021:955). Kommunen är skyldig att vidta skyddsåtgärder för att hantera hot mot Sveriges säkerhet, spioneri, sabotage, terrorism och andra antagonistiska hot. Denna riktlinje fastställer de procedurer och ansvarsfördelningar som ska gälla för att upprätthålla säkerhetsskydd i kommunen.

Syftet med riktlinjen är att skapa ett heltäckande dokument som säkerställer att kommunen följer säkerhetsskyddslagstiftningen.

Riktlinjen anger principer för att skydda säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter samt för att tydliggöra ansvarsområden och organisation.

## 2. Säkerhetsskyddsorganisation och ansvar

### *Kommunstyrelsen*

Kommunstyrelsen har det övergripande ansvaret för att säkerställa att säkerhetsskyddet i kommunen fungerar i enlighet med lagar och förordningar.

### *Säkerhetsskyddschef*

Säkerhetsskyddschefen har ansvar för att leda och samordna säkerhetsskyddsarbetet.

Säkerhetsskyddschefens uppdragsbeskrivning och mandat fastställs av kommunstyrelsens ordförande och kommundirektör.

Denne ska:

- Utföra säkerhetsskyddsbedömningar och se till att riktlinjer och procedurer följs.
- Fungera som kontaktperson gentemot Säkerhetspolisen.
- Genomföra regelbundna kontroller och uppföljningar av säkerhetsskyddsarbetet.
- Ansvara för utbildning och fortbildning av säkerhetsskyddsrutiner för berörd personal.
- Fastställer förvaltningsövergripande rutiner som krävs för att säkerställa efterlevnad av lagar, föreskrifter och interna riktlinjer för säkerhetsskyddsarbetet.

### *Kommundirektör, avdelningschefer, verksamhetschefer och VD för kommunala bolag.*

Kommundirektör, avdelningschefer, verksamhetschefer och VD för kommunala bolag har ansvar för säkerheten inom sin verksamhet. Det innebär att säkerställa att tillräckliga resurser finns och att alla



säkerhetsskyddsåtgärder implementeras enligt säkerhetsskyddschefens rutiner.

### **3. Säkerhetsskyddsanalys och säkerhetsskyddsplan**

#### *Säkerhetsskyddsanalys*

En säkerhetsskyddsanalys ska identifiera vilka uppgifter och verksamheter som är skyddsvärda, samt vilka risker och sårbarheter som finns. Säkerhetsskyddsanalysen fastställs av kommundirektör.

Detta arbete ska innefatta:

- Identifiering av säkerhetshot och sårbarheter.
- Riskbedömning och konsekvensanalys, där varje hot analyseras utifrån dess potentiella inverkan på Sveriges säkerhet.
- Dokumentation och klassificering av säkerhetsskyddsklassificerade uppgifter enligt nivåerna "kvalificerat hemlig," "hemlig," "konfidentiell" och "begränsat hemlig."

#### *Säkerhetsskyddsplan*

Utifrån analysen ska en säkerhetsskyddsplan upprättas. Säkerhetsskyddsplanen fastställs av säkerhetsskyddschefen och regelbundet uppdateras för att återspegla förändringar i hotbild och organisationens struktur.

Planen ska:

- Specificera skyddsåtgärder för säkerhetskänslig verksamhet, information och anläggningar.
- Ange ansvariga personer för varje åtgärd samt tidsramar för genomförande.

### **4. Informationssäkerhet**

Informationssäkerheten ska skydda känsliga uppgifter från obehörig åtkomst, förstörelse och manipulation.

Informationssäkerhet omfattar både administrativ säkerhet och IT-säkerhet:

#### *Administrativ säkerhet*

Administrativ säkerhet säkerställer korrekt hantering av sekretessbelagda dokument.



Följande åtgärder ska vidtas:

- Samtliga säkerhetsskyddsklassificerade handlingar ska registreras och förvaras i säkra utrymmen.
- Endast behörig personal ska få tillgång till information baserat på säkerhetsprövning och arbetsbehov.
- Handlingar ska märkas med sekretessgrad och hanteras enligt fastställda procedurer för att undvika obehörigt röjande.

### *IT-säkerhet*

IT-säkerhet avser att skydda elektroniska informationssystem och data från obehörig åtkomst, ändringar eller förstöring:

- Säkerhetsåtgärder, såsom brandväggar och kryptering, ska finnas för IT-system som innehåller säkerhetsskyddsklassificerade uppgifter.
- Begränsad åtkomst till system via säkra inloggningsmetoder och regelbundna säkerhetsuppdateringar.
- Speciell säkerhetsdator ska användas för att hantera säkerhetsskyddade uppgifter. Uppkoppling till internet eller andra externa nätverk är strikt förbjudet för dessa system.

## **5. Fysisk säkerhet**

Fysisk säkerhet skyddar känsliga områden och utrustning från obehörigt tillträde och skadlig inverkan.

Följande åtgärder är obligatoriska:

- Endast behöriga personer ska ha tillträde till säkerhetskänsliga områden.
- Säkerhetskänsliga platser ska ha övervakning, larm och i vissa fall kameraövervakning för att upptäcka obehörig åtkomst.
- Skyddade zoner ska definieras i säkerhetsskyddsplanen och övervakas med hjälp av lås, larm och begränsat tillträde.

## **6. Personalsäkerhet**

Personalsäkerhet innebär att prövningar görs av anställdas och leverantörers pålitlighet samt att säkerhetsklassning används vid behov:

- Säkerhetsprövning: Alla anställda och personer som arbetar med säkerhetsskyddade uppgifter ska genomgå en säkerhetsprövning innan de får tillgång till sådana uppgifter. Prövningen omfattar bakgrundskontroll och utvärdering av lämplighet.



- Säkerhetsklassning: Positioner med säkerhetskänsliga uppgifter ska klassificeras. Endast personer som godkänts efter prövning får inneha säkerhetsklassade positioner.
- Utbildning i säkerhetsskydd: Personer i säkerhetskänsliga positioner ska genomgå utbildning och kontinuerlig fortbildning i säkerhetsskyddsfrågor.

## 7. Säkerhetsskyddad Upphandling (SUA)

Vid upphandling av tjänster eller produkter som kan påverka kommunens säkerhetsskydd ska särskilda försiktighetsåtgärder vidtas:

- Kommunen ska ingå säkerhetsskyddsavtal med leverantörer som hanterar säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet.
- Vid säkerhetsskyddad upphandling ska leverantören genomgå en säkerhetsprövning för att säkerställa att de följer gällande säkerhetsstandarder och rutiner.
- Säkerhetsskyddschefen ska regelbundet följa upp att leverantören efterlever säkerhetsskyddsavtalet och rapportera eventuella brister.

## 8. Incidenthantering

En robust incidenthanteringsplan ska vara på plats för att omedelbart kunna reagera på säkerhetsincidenter:

- Samtliga säkerhetsincidenter ska rapporteras till säkerhetsskyddschefen, som ansvarar för att utreda och dokumentera händelsen.
- Efter en incident ska säkerhetsskyddschefen vidta omedelbara åtgärder för att minimera riskerna och förhindra framtida incidenter.
- Incidentrapporter och åtgärder ska sparas och användas som underlag för att kontinuerligt förbättra säkerhetsarbetet.

## 9. Utbildning och uppföljning

Regelbunden utbildning och uppföljning är nödvändig för att säkerställa att säkerhetsskyddet hålls aktuellt:

- Utbildning för personal: All personal som arbetar med säkerhetskänslig verksamhet ska genomgå utbildning i säkerhetsskydd, inklusive nya lagkrav och uppdaterade rutiner.
- Årlig uppföljning: Säkerhetsskyddschefen ansvarar för att årligen följa upp säkerhetsskyddet och rapportera resultat och eventuella förbättringsbehov till kommunstyrelsen.



- Revidering av säkerhetsskyddsplan:  
Säkerhetsskyddsplanen ska revideras vid förändringar i verksamheten eller vid nya identifierade hot.