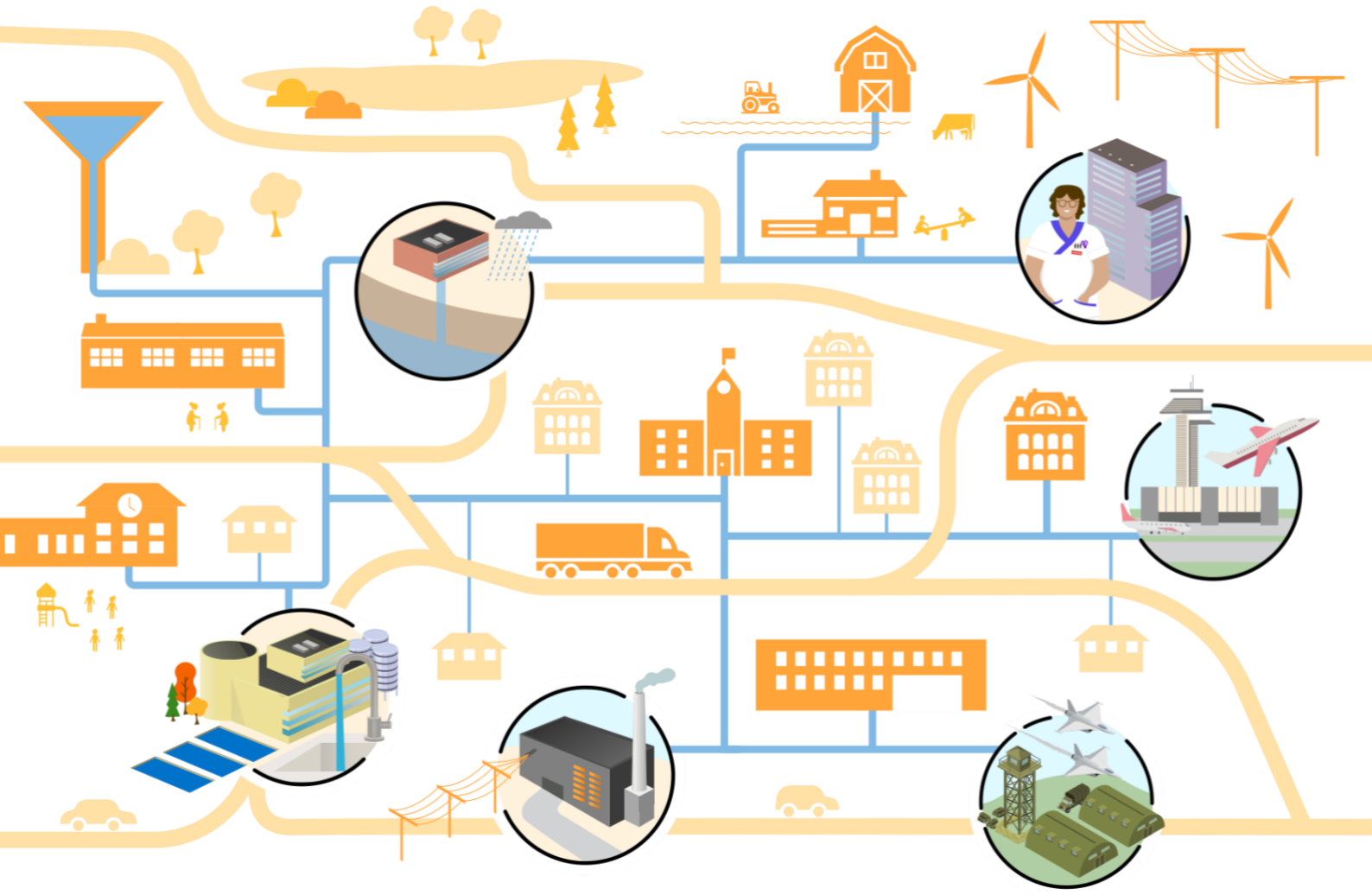
Handbok i krisberedskap och civilt försvar för dricksvatten

Modul 4. Informationssäkerhet, personalsäkerhet och fysisk säkerhet



Livsmedelsverket

Denna titel kan laddas ner från: Livsmedelsverkets publikationer

Rekommenderad citering: Livsmedelsverket, 2023. Uppsala.

Illustrationer av Matador Kommunikation AB.

Om handboken

Handboken för krisberedskap och civilt försvar inom dricksvatten vänder sig i första hand till producenter och distributörer av dricksvatten. Den syftar till att ge praktiskt stöd i arbetet med att skapa en robust och säker dricksvattenförsörjning, samt en god förmåga att hantera störningar och kriser både i fredstid och vid höjd beredskap.

Livsmedelsverket har tagit fram handboken tillsammans med representanter från dricksvattenaktörer, länsstyrelser, statliga myndigheter och branschorganisationen Svenskt Vatten.

Handboken använder begreppet **dricksvattenaktör**, vilket omfattar både **producenter** och **distributörer** av dricksvatten.

Handboken består av följande sju fristående moduler:

1. Krisberedskap och totalförsvarsplanering
2. Hotbild och planeringsförutsättningar
3. Robust dricksvattenförsörjning
4. Informationssäkerhet, personalsäkerhet och fysisk säkerhet
5. Ledning, samverkan och kriskommunikation
6. Externa aktörer och stödresurser
7. Utbildning och övning

Den här modulen, *Informationssäkerhet, personalsäkerhet och fysisk säkerhet*, beskriver hur dricksvattenaktörer kan arbeta med de olika delarna inom säkerhet. Modulen vänder sig till dig som vill ha en övergripande beskrivning av säkerhetsområdet. Modulen innehåller även checklistor och exempel som kan vara till praktisk nytta.

I handboken används två fiktiva organisationer för att ge exempel på hur en dricksvattenaktör kan arbeta i praktiken med de olika frågorna:

Teknik och fastighetsförvaltningen i Grusstads kommun

Grusstad är en medelstor kommun och ingår i Bergslands län. Teknik- och fastighetsförvaltningen ansvarar för dricksvatten i kommunen samt för avlopp, mark, park och kommunens fastigheter.

Dricksvattenförsörjningen baseras på uttag av vatten från en grundvattentäkt och dricksvattnet produceras i ett större grundvattenverk. I kommunen finns även hög- och lågreservoarer samt tryckstegringsstationer. Teknik- och fastighetsförvaltningen sköter drift och underhåll av både anläggningar och ledningsnät med egen personal.

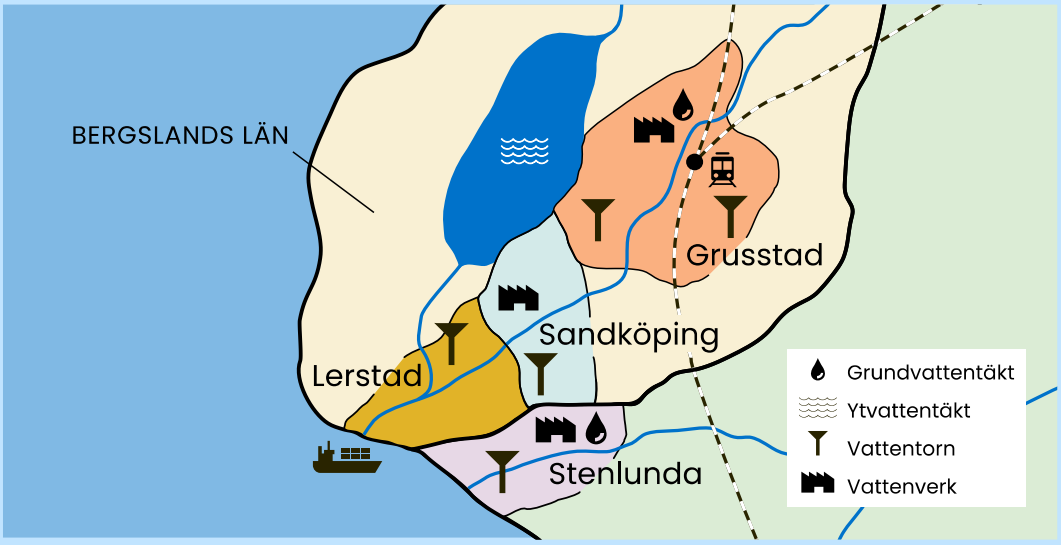
Grusstads kommun är en nationell järnvägsknutpunkt, har ett militärt regemente och ligger inom översvämningskarterat område.

Kommunala bolaget Sandköpings vatten och avfall AB

De tre mindre kommunerna Sandköping, Lerstad och Stenlunda har tillsammans bildat ett kommunalt bolag med ansvar för vatten, avlopp och avfallshantering. Sandköpings och Lerstads kommuner ligger i Bergslands län, medan Stenlunda kommun ligger i ett annat län.

Bolaget har en ytvattentäkt som huvudvattentäkt och en grundvattentäkt som reservvatten. Förutom vattenverk har kommunerna flera hög- och lågreservoarer samt tryckstegringsstationer. Kommunerna har även ett gemensamt sammanbyggt ledningsnät. Sandköpings vatten och avfall AB sköter drift och underhåll av alla anläggningar i egen regi, men har ramavtal med en driftsentreprenör som sköter drift och underhåll av ledningsnätet.

I Lerstad finns en hamn som är en nationellt viktig logistiknod.



Innehåll

Ordlista 7
Informationssäkerhet, personalsäkerhet och fysisk säkerhet – tre viktiga områden för en robust dricksvattenförsörjning 9
Systematiskt säkerhetsarbete 9
Incidenthantering 10
Lagstiftning 12
Vilka verksamheter omfattas av offentlighets- och sekretesslagen? 13
Vilka verksamheter omfattas av Livsmedelsverkets föreskrifter om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar? 13
Vilka verksamheter omfattas av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster? 13
Vilka verksamheter omfattas av säkerhetsskyddslagen? 14
Informationssäkerhet 16
Systematiskt arbete med informationssäkerhet 17
Stöd i det systematiska informationssäkerhetsarbetet 17
Informationsklassning 18
Informationssäkerhet inom ramarna för offentlighets- och sekretesslagen 18
Sekretessbedömning och utlämnande av allmän handling 20
Informationssäkerhet inom ramarna för lås och bom-föreskriften 20
Informationssäkerhet inom ramarna för NIS-lagstiftningen 20
Informationssäkerhet inom ramarna för säkerhetsskyddslagstiftningen 22
Säkerhetskyddsklassificerade uppgifter 22
Säkerhetsskydd av informationssystem 25
Personalsäkerhet 27
Systematiskt arbete med personalsäkerhet 29
Vid rekrytering 29
Under anställning 30
När en anställning ska upphöra 30
Extern personal 30
Personalsäkerhet inom ramarna för säkerhetsskyddslagstiftningen 31
Utbildning 31
Placering i säkerhetsklass 31
Säkerhetsprövning 34
Extern personal i säkerhetskänslig verksamhet 36

Fysisk säkerhet....37
Systematiskt arbete med fysisk säkerhet....40
Åtgärder för att upptäcka, försvåra och hantera....41
Skyddsobjekt....43
Hot och våld mot personal....44
Fysisk säkerhet inom ramarna för lås och bom-föreskriften....44
Fysisk säkerhet inom ramarna för säkerhetsskyddslagstiftningen....44
Upphandling....46
Upphandling med sekretess- och säkerhetsavtal....46
Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)....48
Säkerhetsskyddsöverenskommelse....49
Bilaga 1. Stöd vid sekretessbedömning och utlämnande av allmän handling
Bilaga 2. Exempel – uppgifter inom dricksvattenförsörjning som kan omfattas av sekretess
Bilaga 3. Exempel – intervjufrågor vid säkerhetsintervju
Bilaga 4. Exempel – sekretessförbindelse
Bilaga 5. Exempel – Sandköping vatten och avfall AB:s tillträdesrutin

Ordlista

Fysisk säkerhet

Fysisk säkerhet är ett system bestående av personal, rutiner, byggnads- och säkerhetsteknik som tillsammans upptäcker, försvårar och hanterar obehörigt tillträde och skadlig inverkan.

Informationsklassning

Informationsklassning innebär att identifiera skyddsbehovet för en viss typ av information utifrån en konsekvensanalys.

Informationssäkerhet

Informationssäkerhet handlar om att skydda information avseende konfidentialitet, riktighet och tillgänglighet. Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk som rutiner och riktlinjer, tekniskt skydd som till exempel brandväggar och kryptering samt fysiskt skydd som till exempel skal- och brandskydd.

Myndighet

Myndighet avser i denna handbok samtliga statliga och kommunala organ med undantag för beslutande politiska församlingar. Myndighet avser alltså såväl kommunala förvaltningar som kommunala bolag och kommunalförbund.

NIS-reglering

NIS-regleringen utgår från EU-direktivet *2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen* och ställer krav på säkerhet i nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster. För att det europeiska NIS-direktivet ska vara giltigt i svensk rätt har riksdagen beslutat om den svenska NIS-regleringen. Den omfattar bland annat *lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster* samt *förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*.

Personalsäkerhet

Personalsäkerhet används i den här handboken ur två perspektiv. Dels som ett allmänt begrepp som avser åtgärder för att förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en dricksvattenaktörs verksamhet och se till att de som deltar i en dricksvattenaktörs verksamhet har tillräcklig kunskap om verksamhetens säkerhets-rutiner. Dels som ett begrepp i säkerhetsskyddslagstiftningen som avser åtgärder som ska förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i säkerhetskänslig verksamhet och se till att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskyddet.

Röjande av uppgift

Röjande av uppgift innebär att på ett felaktigt sätt sprida uppgifter som omfattas av sekretess.

Sekretess

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

Sekretessreglerad uppgift

En sekretessreglerad uppgift är en uppgift för vilken det finns en bestämmelse om sekretess.

Sekretessbelagd uppgift

En sekretessbelagd uppgift är en uppgift för vilken sekretess gäller i ett enskilt fall.

Säkerhetskänslig verksamhet

Säkerhetskänslig verksamhet är ett begrepp från säkerhetsskyddslagstiftningen. Begreppet avser verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Uttrycket Sveriges säkerhet avser sådant som är av grundläggande betydelse för Sverige, såsom försvaret, det demokratiska statsskicket, rättsväsendet och samhällsviktig verksamhet som är av betydelse ur ett nationellt perspektiv.

Säkerhetsskydd

Säkerhetsskydd är ett begrepp från säkerhetsskyddslagstiftningen. Begreppet avser skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskydds-klassificerade uppgifter. Åtgärderna kan bestå av informationssäkerhet, fysisk säkerhet och personalsäkerhet i kombination.

Verksamhetsbeskrivning

En verksamhetsbeskrivning är det första steget i Säkerhetspolisens modell för att göra en säkerhetsskyddsanalys. Den beskriver verksamheten på ett övergripande plan och identifierar eventuell säkerhetskänslig verksamhet. Verksamhetsbeskrivningen ger därmed svar på om en dricksvattenaktör omfattas av säkerhetsskyddslagen eller inte.

Verksamhetsskydd

Verksamhetsskydd används i handboken som ett samlingsbegrepp för det arbete som bedrivs för att skydda samhällsviktig verksamhet genom att vidta åtgärder inom områdena informationssäkerhet, personalsäkerhet samt fysisk säkerhet och som inte utgör säkerhetsskydd.

Informationssäkerhet, personal-säkerhet och fysisk säkerhet – tre viktiga områden för en robust dricksvattenförsörjning

Produktion och distribution av dricksvatten är en samhällsviktig verksamhet. Det finns en mängd olika händelser som kan hota dricksvattenförsörjningen, både antagonistiska och icke-antagonistiska,. Läs mer om hotbilden i modul 2, *Hotbild och planerings-förutsättningar*.

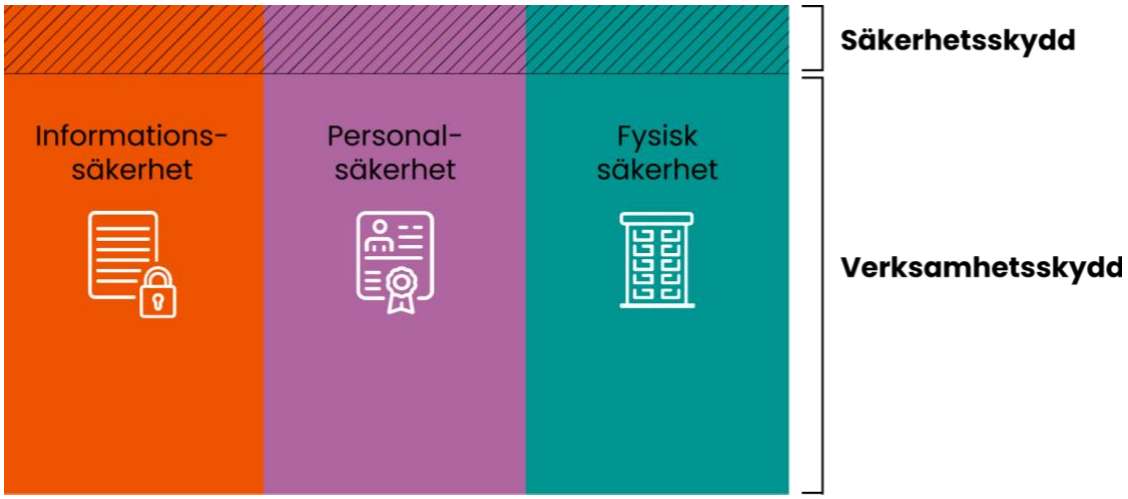
Den här modulen beskriver tre delar inom säkerhetsarbetet som är viktiga för alla dricksvattenaktörer:

- informationssäkerhet
- personalsäkerhet
- fysisk säkerhet.

Säkerhetsarbetet behöver bedrivas systematiskt inom alla dessa tre områden. Utifrån kännedom om verksamhetens skyddsvärden, hot och sårbarheter kan dricksvatten-aktörer utforma rutiner och riktlinjer som styr säkerhetsarbetet. Att förankra säkerhets-arbetet hos ledningen är en avgörande framgångsfaktor.

Systematiskt säkerhetsarbete

Dricksvattenförsörjningen behöver fungera såväl till vardags som vid oönskade händelser. Ett säkerhetsarbete som är anpassat utifrån identifierade hot och risker är en bra grund för att skydda verksamheten. Grunden består av verksamhetens informations-säkerhetsarbete, personalsäkerhetsarbete och arbete med fysisk säkerhet. Dessa tre områden utgör tillsammans dricksvattenaktörens verksamhetsskydd. Utifrån denna grund kan skyddet utökas för de dricksvattenaktörer som omfattas av säkerhetsskydds-lagstiftningen (se figur 1).



Figur 1. Ett systematiskt säkerhetsarbete innefattar informationssäkerhet, personalsäkerhet och fysisk säkerhet och utgör tillsammans verksamhetsskyddet. Säkerhetsskyddet tillkommer för de dricksvattenaktörer som bedriver säkerhetskänslig verksamhet och därmed omfattas av säkerhetsskyddslagen.

Säkerhetsarbetet behöver bedrivas systematiskt för att uppnå bästa effekt. Med **systematiskt** menas bland annat att arbetet

- är strukturerat och metodiskt – det vill säga planeras, följer rutiner och inte sker godtyckligt
- sker med regelbundenhet eller kontinuerligt och är ständigt levande
- dokumenteras för att möjliggöra styrning och uppföljning
- involverar hela verksamheten
- är personoberoende.

Exempel på viktiga moment som kan ingå i det systematiska säkerhetsarbetet är riskanalyser och incidenthantering, se modul 3, *Robust dricksvattenförsörjning* och avsnittet *Incidenthantering*.

Det finns också lagstiftning som berör informationssäkerhet, personalsäkerhet och fysisk säkerhet och som ställer krav på dricksvattenaktören. Dessa krav behöver arbetas in i och utgöra en del av verksamhetens systematiska säkerhetsarbete, se avsnittet *Lagstiftning*.

Incidenthantering

Det är en fördel att tillämpa en i förväg bestämd och inövad process för att hantera säkerhetsrelaterade incidenter. Det finns många olika exempel på sådana processer, bland annat inom ramen för standarder som ISO 27000-serien och IEC 62443. De flesta processer för incidenthantering innehåller de fem stegen förebygga, identifiera, begränsa, återställa och följa upp:

1. **Förebygga**
   Detta är förberedande åtgärder för att exempelvis införa metoder för att upptäcka säkerhetsincidenter, tydliggöra ansvar när det gäller att hantera incidenter samt utforma arbetssätt och rutiner.

2. **Identifiera**
   Detta steg omfattar åtgärder för att samla information och analysera det som har inträffat, för att på så sätt bygga en förmåga att upptäcka säkerhetsincidenter genom exempelvis:
   a. loggrutiner – att logga och hantera varningar (triggers, anomalier)
   b. dricksvattenspecifika larm – felaktiga värden, processhaveri, flöden
   c. inbrottslarm, brandlarm, kamerabevakning
   d. avlyssning av nätverk (loggar)
   e. ovanliga inloggningar
   f. allmänhetens indata.

   När en incident inträffat samlar berörda aktörer information för att kunna analysera händelsen och bedöma vilka åtgärder som ska genomföras. Det kan exempelvis vara att besluta om att stänga ned en tjänst, att övergå till manuell drift, att utfärda en kokningsrekommendation eller att besluta om bräddning av vattentorn. I steget ingår även att klassificera incidenten, att rapportera enligt gällande rutiner samt att genomföra informationsinsatser.

3. **Begränsa**
   Olika typer av åtgärder kan sättas in för att begränsa skadorna av en säkerhets-incident, exempelvis ö-drift eller åtgärder för att stoppa spridning av skadlig kod som till exempel ransomware.

4. **Återställa**
   Den här delen av processen innefattar åtgärder för att återställa till normalläge. Ett exempel är att återställa system från backup eller ominstallationer. Detta kan kräva att verksamheten har gjort prioriteringar på förhand, till exempel genom att fastställa vilka verksamheter och system som ska prioriteras först i återställningsarbetet.

5. **Följa upp**
   Syftet med uppföljning är att lära av erfarenheterna från en inträffad säkerhets-incident. Det sker genom att gå till botten med vad som orsakade incidenten, utvärdera rutinerna och genomföra aktiviteter för att återföra lärdomar till de berörda verksamheterna.

Lagstiftning

En viktig del i säkerhetsarbetet är att analysera vilken lagstiftning som verksamheten omfattas av, exempelvis *offentlighets- och sekretesslagen*[1], Livsmedelsverkets föreskrifter om åtgärder för att förhindra sabotage och annan skadegörelse mot dricksvattenanläggningar, den så kallade lås och bom-föreskriften[2], NIS-lagstiftningen[3] och säkerhetsskyddslagstiftningen[4] (se tabell 1). Dessa författningar styr vilka krav som ställs på säkerhetsarbetet.

Tabell 1. Exempel på olika författningar inom säkerhetsområdet.

Författning	Vilka omfattas?	Område		
		Informations-säkerhet	Personal-säkerhet	Fysisk säkerhet
Offentlighets- och sekretesslagen	Alla kommunala dricksvattenaktörer.	Ja	Nej	Nej
Lås och bom-föreskriften	Kommunala verksamheter med vattenverk och distributionsanläggningar som producerar eller tillhandahåller dricksvatten till fler än 2000 personer.	Ja	Nej	Ja
NIS-lagstiftningen	För leverantörer som tillhandahåller vatten till minst 20 000 personer eller till akutsjukhus.	Ja	Nej	Nej
Säkerhetsskydds-lagstiftningen	Dricksvattenaktörer med säkerhetskänslig verksamhet, det vill säga sådan verksamhet som är av betydelse för Sveriges säkerhet.	Ja	Ja	Ja

[1] Offentlighets- och sekretesslag (2009:400)

[2] LIVSFS 2008:13 Åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar

[3] Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

[4] Bestämmelserna i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955) kompletteras av Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)

Vilka verksamheter omfattas av offentlighets- och sekretesslagen?

Alla offentliga verksamheter omfattas av *offentlighets- och sekretesslagen*. Det innebär att lagen gäller för alla kommunala dricksvattenaktörer.

Vilka verksamheter omfattas av Livsmedelsverkets föreskrifter om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar?

Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar kallas för lås och bom-föreskrifterna. De ska tillämpas på vattenverk och distributionsanläggningar som producerar respektive tillhandahåller dricksvatten till mer än 2 000 personer, och som en kommun har ett rättsligt bestämmande inflytande över. Kommunens verksamhet för miljö och hälsa är kontrollmyndighet.

De delar som rör informationssäkerhet i lås och bom-föreskriften gäller inte för verksamheter som omfattas av *lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*[5].

Vilka verksamheter omfattas av lagen om informations-säkerhet för samhällsviktiga och digitala tjänster?

NIS-lagstiftningen[6] ställer särskilda krav på kommunala dricksvattenaktörer som tillhandahåller dricksvatten till minst 20 000 personer eller till akutsjukhus när det gäller arbete med informationssäkerhet kopplat till nätverk och informationssystem som används för den samhällsviktiga tjänsten.[7] Livsmedelsverket är tillsynsmyndighet för sektorn leverans och distribution av dricksvatten.

NIS-lagstiftningen gäller inte för verksamhet som omfattas av säkerhetsskyddslagen[8]. En dricksvattenaktör skulle i teorin kunna beröras av båda lagstiftningarna för olika

[5] LIVSFS 2022:3 Föreskrifter om ändring i Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar.

[6] Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

[7] MSBFS 2021:9 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster samt MSB, Vägledning för anmälan och identifiering av leverantörer av samhällsviktiga tjänster enligt NIS-regleringen, dnr 2022-03659, 2022.

[8] Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

delar av sin verksamhet, men i praktiken finns det sannolikt få exempel på detta. Det skulle nämligen förutsätta att dricksvattenaktörens industriella informations- och styrsystem omfattas av NIS samtidigt som andra delar av dricksvattenaktörens verksamhet omfattas av säkerhetsskydd.

Vilka verksamheter omfattas av säkerhetsskyddslagen?

En dricksvattenverksamhet kan omfattas av *säkerhetsskyddslagen (2018:585)* med tillhörande förordning och föreskrifter. Det gäller om verksamhetsbeskrivningen visar att dricksvattenaktörens verksamhet är av betydelse för Sveriges säkerhet, och därmed utgör en **säkerhetskänslig verksamhet**.

Sådana verksamheter behöver ett särskilt skydd – säkerhetsskydd – som syftar till att skydda säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter.

Är dricksvattenförsörjning en säkerhetskänslig verksamhet?

Med säkerhetskänslig verksamhet avses sådan verksamhet som är av betydelse för Sveriges säkerhet. Uttrycket Sveriges säkerhet tar sikte på sådant som är av grundläggande betydelse för Sverige. I detta ingår bland annat:

- det militära och civila försvaret
- den nationella ekonomin
- de brottsbekämpande myndigheterna
- domstolarna
- sådana leveranser av exempelvis livsmedel, elkraft, dricksvatten och drivmedel som är nödvändiga för samhällets funktionalitet på nationell nivå.[9]

Samhällsviktig verksamhet är inte samma sak som **säkerhetskänslig verksamhet**. Många samhällsviktiga verksamheter omfattas inte av bestämmelserna om säkerhets-skydd. Det finns ingen förteckning över vilka verksamheter som omfattas av säkerhetsskyddslagen, utan det är dricksvattenaktören själv som ansvarar för att göra bedömningen genom att genomföra en säkerhetsskyddsanalys.[10]

Säkerhetskänsliga kommunala verksamheter ska anmälas till någon av de tillsyns-ansvariga länsstyrelserna (Skåne, Västra Götaland, Stockholm eller Norrbotten). Det är även dessa länsstyrelser som är tillsynsmyndighet för säkerhetskänsliga kommunala dricksvattenverksamheter, oavsett driftsform.

[9] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd*, 2019.

[10] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys*, 2023.

Dricksvattenaktörer kan bedriva säkerhetskänslig verksamhet och därmed omfattas av säkerhetsskyddslagen. Den verksamhetsbeskrivning som genomförs kommer att visa vilka delar av verksamheten som omfattas av säkerhetsskyddslagstiftningen. Verksamhetsbeskrivningen ska svara på om en antagonistisk handling mot dricksvatten-verksamheten, eller ett röjande av uppgifter om verksamheten, skulle kunna medföra konsekvenser som leder till skada för Sveriges säkerhet.

Exempel på dricksvattenverksamheter som skulle kunna bedömas som säkerhets-känsliga är de som försörjer samhällsviktiga verksamheter av nationellt intresse och som är beroende av en fungerande dricksvattenförsörjning för att upprätthålla sin verksamhet. För att dricksvattenaktören ska kunna göra rätt bedömning är det viktigt att ha en dialog med de samhällsviktiga verksamheter som dricksvattenaktören försörjer med dricksvatten.

Informationssäkerhet

Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning. Informationssäkerhet handlar om att skydda information så att:

- endast behöriga personer får ta del av den (konfidentialitet)
- den är korrekt och inte manipulerad eller förstörd (riktighet)
- den alltid finns när den behövs (tillgänglighet).

Faktaruta: Tre centrala begrepp inom informationssäkerhet

Konfidentialitet

Konfidentialitet innebär att information bara ska vara tillgänglig för de som har behörighet att ta del av den och som har behov av informationen för att kunna utföra sitt arbete.

Riktighet

Riktighet innebär att information alltid ska vara korrekt och inte kunna ändras av obehöriga, av misstag eller av en funktionsstörning i systemet som hanterar informationen.

Tillgänglighet

Tillgänglighet innebär att informationen alltid ska finnas tillgänglig när den behövs. I en dricksvattenverksamhet kan det även handla om att de industriella informations- och styrsystem som används i dricksvattenproduktionen alltid ska vara tillgängliga.

Dricksvattenaktörer har en stor mängd information kopplat till produktion och distribution av dricksvatten. Informationens tillgänglighet och riktighet är avgörande för möjligheten att bedriva verksamheten. Det kan till exempel vara information i form av:

- drift- och skötselinstruktioner
- ritningar och processbeskrivningar
- GIS-data
- kris- och beredskapsplaner.

Denna information kan också utgöra redskap för någon som med ont uppsåt vill utföra sabotage eller annan skada riktad mot dricksvattenförsörjningen. Det är därför viktigt att alla dricksvattenaktörer arbetar systematiskt med informationssäkerhet.

Systematiskt arbete med informationssäkerhet

Systematiskt informationssäkerhetsarbete innebär att arbeta förebyggande och att kontinuerligt anpassa skyddet utifrån organisationens behov och risker. Arbetet med informationssäkerhet omfattar bland annat att införa och förvalta:

- administrativa regelverk så som rutiner och riktlinjer
- tekniskt skydd med bland annat brandväggar och kryptering
- fysiskt skydd med till exempel skal- och brandskydd.

Ett systematiskt arbete med informationssäkerhet kräver att ledningen är engagerad i arbetet, samt att ledningen avsätter både tid och resurser till arbetet. En förutsättning för att lyckas är att utse en ansvarig för informationssäkerhetsarbetet som leder och driver arbetet. Riktlinjer för informationssäkerhetsarbetet med tillhörande rutiner ger också stöd och beslutsunderlag till verksamheten. Exempel på frågor som sådana rutiner kan besvara är:

- I vilka system får sekretessreglerad information hanteras?
- Får man diskutera sekretessreglerad information på videomöten?
- Vilka hanteringsregler gäller för olika sekretesstyper?
- Till vilka system och i vilka situationer krävs tvåfaktorsinloggning?
- För vilka system krävs separata nätverk?
- Hur och när ska säkerhetsuppdateringar installeras?
- Hur ska pärmar, papperskopior och utskrivna ritningar förvaras?

En viktig del i arbetet med informationssäkerhet är att informera, utbilda och öva personalen i organisationens rutiner och riktlinjer. Dricksvattenaktören behöver regelbundet följa upp åtgärder och hur väl rutiner följs. Uppföljningen ger underlag till beslut om nya åtgärder eller justeringar av styrande dokument och rutiner.

Stöd i det systematiska informationssäkerhetsarbetet

Dricksvattenaktörer kan utgå från etablerade standarder i arbetet med informations-säkerhet för att få en god struktur i sitt eget arbete. MSB har tagit fram ett metodstöd kring systematiskt informationssäkerhetsarbete som syftar till att förtydliga hur ett systematiskt informationssäkerhetsarbete kan utformas. Metodstödet består av fyra steg och bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien. Materialet i sin helhet finns på den av MSB administrerade webbplatsen www.informationssäkerhet.se via Metodstöd för LIS (informationssakerhet.se).

MSB erbjuder även en rådgivningstjänst dit exempelvis dricksvattenaktörer kan vända sig för att få råd och stöd när det gäller det förebyggande arbetet med informationssäkerhet. Rådgivning kan bokas via MSB:s webb Rådgivningstjänst för systematiskt informationssäkerhetsarbete (msb.se).

Informationsklassning

En viktig del i det systematiska arbetet med informationssäkerhet är att klassa verksamhetens information. Det innebär att informationen värderas utifrån vilka konsekvenser som ett otillräckligt skydd skulle kunna få med hänsyn till de tre parametrarna konfidentialitet, riktighet och tillgänglighet. Klassningen identifierar skyddsbehovet för informationen.

Klassning av information görs lämpligtvis i samband med att informationen skapas. Det kan också vara lämpligt att göra någon form av återkommande översyn för att kontrollera att informationsklassningen fortfarande är på rätt nivå.

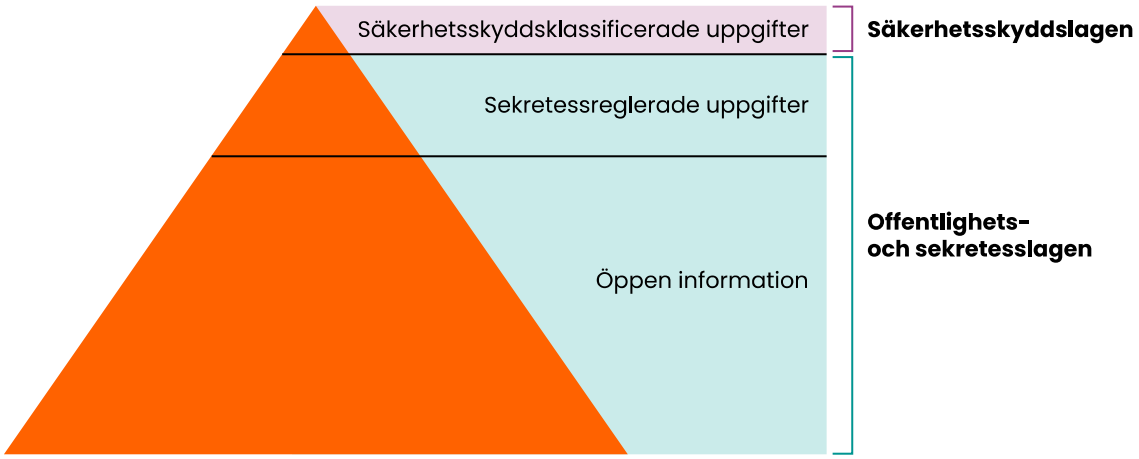
Tips!

Sveriges kommuner och regioner (SKR) har tagit fram ett stödmaterial samt ett verktyg för informationsklassning. Läs mer här: KLASSA, informationsklassning | SKR

Myndigheten för samhällsskydd och beredskap (MSB) driver webbplatsen www.informationssäkerhet.se. Där finns bland annat vägledning kring informationsklassning Informationssäkerhet.se – Klassning av information.

Informationssäkerhet inom ramarna för offentlighets- och sekretesslagen

Den största delen av en dricksvattenaktörs information är öppen, medan en mindre del av informationen omfattas av sekretess. Men bara för att information är öppen innebär det inte att den måste – eller är lämplig – att publicera på webben. För dricksvattenaktörer som bedriver säkerhetskänslig verksamhet kan viss information vara säkerhetsskyddsklassificerade uppgifter. Informationen omfattas av olika lagstiftningar (se figur 2).



Figur 2. Den största andelen information är öppen, endast en liten del av informationen omfattas av sekretess. För de som bedriver säkerhetskänslig verksamhet kan viss information vara säkerhetsskyddsklassificerade uppgifter.

Enligt offentlighetsprincipen ska myndigheternas arbete bedrivas i öppna former med insyn från allmänhet och media. Tryckfrihetsförordningen (1949:105) anger att var och en har rätt att ta del av allmänna handlingar. Information som rör alla offentliga verksamheter, till exempel kommunal dricksvattenförsörjning, ska i regel vara tillgänglig för alla. Med det finns vissa begränsningar i rätten att ta del av allmänna handlingar. Under vissa omständigheter omfattas uppgifter i myndigheternas allmänna handlingar av sekretess. Med myndigheter avses även kommunala bolag och kommunalförbund[11].

Det finns olika grunder för att en uppgift ska vara sekretessbelagd, exempelvis sekretess för affärs- och driftförhållanden eller sekretess för uppgifter som rör upphandling. I *offentlighets- och sekretesslagen* finns även ett antal sekretessbestämmelser som rör krisberedskap och totalförsvar:

- försvarssekretess enligt 15 kap. 2 §
- säkerhets- och bevakningsåtgärd enligt 18 kap. 8 §
- risk- och sårbarhetsanalyser m.m. enligt 18 kap. 13 §.

[11] 2 kap. 2 § offentlighets- och sekretesslagen (2009:400).

Sekretessbedömning och utlämnande av allmän handling

Vem som helst, svensk eller utländsk medborgare, har rätt att ta del av allmänna handlingar. Vid begäran om utlämnande av allmän handling får dricksvattenaktören inte efterforska varför personen vill ta del av handlingen, vem personen är eller vad personen ska ha handlingarna till. Om uppgifter i handlingen omfattas av sekretess kan dricksvattenaktören däremot under sekretessbedömningen fråga efter personens identitet och varför personen vill ta del av handlingen, för att kunna göra en korrekt sekretess-bedömning. Se vidare i bilaga 1 *Stöd vid sekretessbedömning och utlämnande av allmän handling*.

Det är den myndighet som förvarar en uppgift som bedömer uppgiftens skyddsvärde. I bilaga 2 finns ett stödmaterial med exempel på uppgifter inom dricksvattenverksamhet som **kan** omfattas av sekretess. Där finns även exempel på uppgifter som **sannolikt inte** omfattas av sekretess. Det är viktigt att varje aktör gör sin egen bedömning i varje enskilt fall.

Informationssäkerhet inom ramarna för lås och bom-föreskriften

Enligt Livsmedelsverkets så kallade lås och bom-föreskrifter ska system för drift och övervakning av dricksvattenproduktion och -distribution skyddas mot obehörig åtkomst. Detsamma gäller handlingar som är av betydelse för dricksvattenproduktion och -distribution.[12]

Informationssäkerhet inom ramarna för NIS-lagstiftningen

De dricksvattenaktörer som omfattas av NIS-regleringen måste bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ISO 27000-seriens standarder eller motsvarande.[13] Det ställs även krav på att bland annat genomföra riskanalyser, ta fram åtgärdsplaner baserade på genomförda riskanalyser och genomföra vissa

[12] Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar LIVSFS 2008:13 (livsmedelsverket.se).

[13] Myndighetens för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informations-säkerhet för leverantörer av samhällsviktiga tjänster.

grundläggande säkerhetsåtgärder.[14] Kraven för dricksvattenaktörer som omfattas av NIS-lagstiftningen beskrivs mer detaljerat på Livsmedelsverkets webbplats Krav och föreskrifter (livsmedelsverket.se) och i vägledningen till Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn produktion och distribution av dricksvatten.[15] Om hantering av nätverk och informationssystem har kontrakterats till externa aktörer så omfattas även dessa aktörer av kraven. Dricksvatten-aktören är då ansvarig för att de externa aktörerna följer kraven.

De som omfattas av NIS-regleringen ska även rapportera incidenter som orsakar störningar i nätverk och informationssystem med betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten till MSB. Aktörer inom leverans och distribution av dricksvatten ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

- har pågått i minst två timmar och som
  - kan antas ha påverkat minst 2 000 personer
  - har påverkat akutsjukhus, eller
- har påverkat styrning och övervakning av tjänsten.[16]

Läs mer om incidentrapportering och detaljer kring hur, när och vad som ska rapporteras på MSB:s webb[17] eller i MSB:s vägledning, *Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen* (dnr MSB 2018-13470).

[14] Livsmedelsverkets föreskrifter (2022:2) om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten.

[15] Livsmedelsverket (2023) *Vägledning till Livsmedelsverkets föreskrifter om informationssäkerhets-åtgärder för samhällsviktiga tjänster inom sektorn produktion och distribution av dricksvatten*.

[16] MSBFS 2018:9 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster.

[17] MSB (2022). Incidentrapportering för leverantörer av samhällsviktiga tjänster. Hämtad 2022-11-06 från Incidentrapportering för leverantörer av samhällsviktiga tjänster (msb.se).

Informationssäkerhet inom ramarna för säkerhetsskyddslagstiftningen

De dricksvattenaktörer som bedriver säkerhetskänslig verksamhet måste uppfylla särskilda krav med avseende på informationssäkerhet. Säkerhetsskyddslagen säger att säkerhetsskyddsåtgärden informationssäkerhet ska:

1. förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och
2. förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

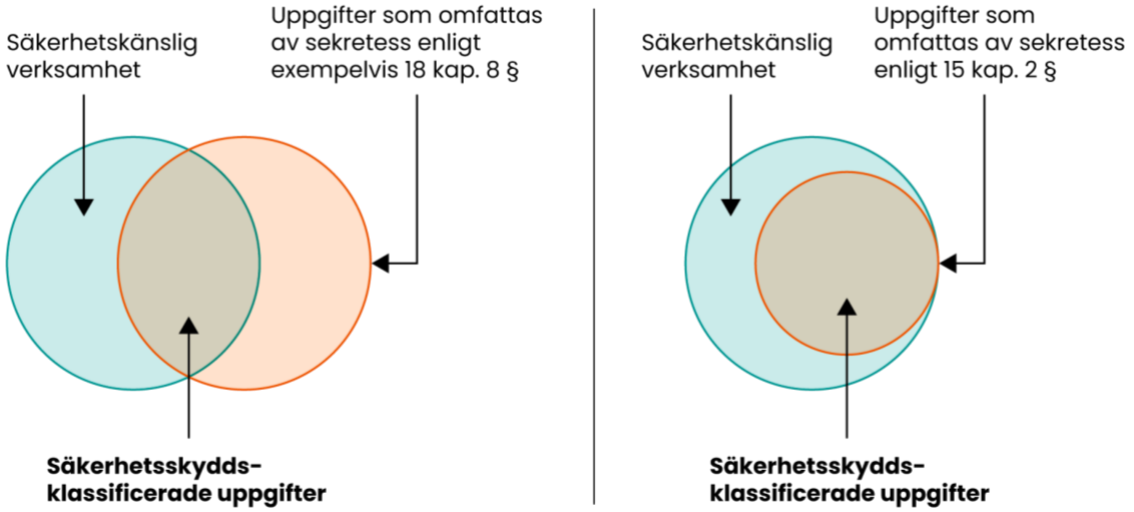
It-incidenter som omfattas av 2 kap. 4 § punkt 2 i *säkerhetsskyddsförordningen (2021:955)* ska skyndsamt anmälas till Säkerhetspolisen.

Mer detaljerade bestämmelser finns i Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1). Säkerhetspolisen har som komplement till föreskrifterna även tagit fram en vägledning om hur säkerhetsskyddsåtgärder inom informationssäkerhet kan utformas, *Vägledning i säkerhetsskydd – Informationssäkerhet.*[18]

Säkerhetskyddsklassificerade uppgifter

I säkerhetsskydd ingår att skydda uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt *offentlighets- och sekretesslagen* (OSL). Uppgifter som omfattas av OSL 15 kap. 2 § är **alltid** säkerhetsskyddsklassificerade uppgifter, medan uppgifter som omfattas av OSL 18 kap. 8 § och 13 § **kan** vara säkerhetsskyddsklassificerade (se figur 3).

[18] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Informationssäkerhet*, 2020.



Figur 3. Relationen mellan säkerhetskänslig verksamhet, säkerhetsskyddsklassificerade uppgifter och sekretess enligt offentlighets- och sekretesslagen.

Dricksvattenaktörer behöver kunna göra en sekretessbedömning för att kunna bedöma om en uppgift är **säkerhetsskyddsklassificerad**. Säkerhetsskyddsklassificerade uppgifter ska delas in i fyra säkerhetsskyddsklasser, utifrån vilken skada för Sveriges säkerhet som kan uppstå om de röjs (se tabell 2).[19]

[19] Säkerhetspolisens webbplats, informationen hämtad 2022-10-26. Om säkerhetsskydd – Säkerhetspolisen (sakerhetspolisen.se).

Tabell 2. Fyra säkerhetsskyddsklasser, ur Säkerhetspolisens vägledning.[20]

Säkerhetsskyddsklass	Den skada som ett röjande av uppgifterna kan medföra	Värdeord till stöd för bedömningen om en viss typ av skada föreligger
Kvalificerat hemlig	Ett röjande kan medföra en synnerligen allvarlig skada.	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig	Ett röjande kan medföra en allvarlig skada.	Allvarliga/betydande negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Konfidentiell	Ett röjande kan medföra en inte obetydlig skada.	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig	Ett röjande kan medföra endast ringa skada.	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.

För att bedöma vilken skada som kan uppstå för Sveriges säkerhet om uppgifterna röjs behöver dricksvattenaktörer fundera på vilka konsekvenser ett röjande kan få. Säkerhetspolisen ger flera tips i *Vägledning i säkerhetsskydd – Informationssäkerhet*:

- Beakta **inte** konsekvenser av ett röjande som framstår som helt orimliga.
- Gör en bedömning utifrån vad som är det värsta **rimliga** scenariot om uppgifterna röjs.
- **Undvik** att ta höjd för vad som skulle hända om andra uppgifter skulle röjas vid samma tidpunkt. Indelningen i säkerhetsskyddsklasser riskerar då att leda till att i princip samtliga uppgifter delas in i någon av de högre klasserna, vilket inte är syftet med lagstiftningen.

[20] Säkerhetspolisen, Vägledning i säkerhetsskydd – Informationssäkerhet, 2020.

För att en uppgift ska delas in i en säkerhetsskyddsklass krävs att de negativa konsekvenserna vid ett röjande påverkar den nationella förmågan. Med nationell förmåga avses till exempel den nationella försvarsförmågan, den nationella elförsörjningsförmågan, den nationella betalningsförmågan eller leverans av dricksvatten som är nödvändig för att upprätthålla samhällets funktionalitet på nationell nivå.[21]

Om en aktör bedömer att det finns säkerhetsskyddsklassificerade uppgifter i verksamheten finns detaljerade hanteringsregler i Säkerhetspolisens *Vägledning i säkerhetsskydd – Informationssäkerhet*.

Säkerhetsskydd av informationssystem

Säkerhetsskyddsåtgärden informationssäkerhet ska både skydda säkerhetsskyddsklassificerade uppgifter och skydda själva informationssystemen som har betydelse för den säkerhetskänsliga verksamheten. Eventuella reservrutiner kopplat till dessa system ska också skyddas.

Informationssystem är system av sammansatt mjuk- och hårdvara som behandlar information. Skyddsåtgärder för informationssystem tar framför allt sikte på att tillgodose behovet av tillgänglighet och riktighet. Vilka åtgärder som är motiverade att genomföra ska analyseras och bedömas i verksamhetens säkerhetsskyddsanalys, samt i förekommande fall i ett informationssystems särskilda säkerhetsskyddsbedömning.

[21] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Informationssäkerhet*, 2020 och *Introduktion till säkerhetsskydd*, 2019.

Vill du läsa mer?

Livsmedelsverkets webbplats om Säkra nätverk och informationssystem för dricksvatten (NIS) (livsmedelsverket.se)

Livsmedelsverket (2023). Vägledning till Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn produktion och distribution av dricksvatten

MSB:s webbplats om NIS-direktivet (msb.se)

MSB (2018). Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen (msb.se)

Säkerhetspolisens information, föreskrifter och vägledningar

En stor del av Säkerhetspolisens *Vägledning i säkerhetsskydd – Informationssäkerhet* siktar särskilt på att utgöra ett stöd i hur berörda aktörer i praktiken kan tillämpa bestämmelserna om informationssäkerhet i informationssystem. Även tillsyns-myndigheten kan fungera som ett stöd till dricksvattenaktören.

Personalsäkerhet

Det är viktigt att alla som bedriver verksamhet inom dricksvattenförsörjning analyserar och genomför åtgärder som minskar risken för att personer som inte är pålitliga ur säkerhetssynpunkt får tillgång till sekretessreglerad information, behörighet till industriella informations- och styrsystem eller tillträde till dricksvattenanläggningar. För dricksvattenaktörer kan det exempelvis handla om tillgång till nödvattenplaner, instruktioner, kartmaterial, information om ledningsnät, passerkort och nycklar. Rutiner för personalsäkerhet behöver gälla för egen anställd personal, konsulter, entreprenörer och kontroll- och tillsynspersonal.

Det är viktigt att bygga en säkerhetskultur där personalen tänker på säkerhet som en naturlig del av arbetet och där det är enkelt och tillåtande att anmäla avvikelser och incidenter. En annan del i personalsäkerhetsarbetet är att säkerställa att den personal som har tillgång till sekretessreglerad information eller dricksvattenanläggningar har tillräcklig kunskap inom säkerhet, till exempel om verksamhetens säkerhetsrutiner och riktlinjer. Säkerhetsutbildning för chefer, medarbetare, konsulter och entreprenörer är därför en central del av en dricksvattenaktörs säkerhetsarbete. Se modul 7, *Utbildning och övning* för exempel på olika roller och befattningars utbildningsbehov.

Exempel: Säkerhetsutbildning i Grusstads kommun

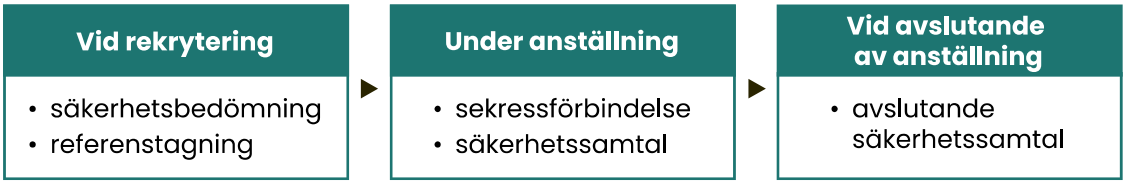
All personal och alla entreprenörer som arbetar med dricksvattenproduktion och -distribution inom Grusstads Teknik- och fastighetsförvaltning genomgår regelbundet en säkerhetsutbildning. Förvaltningen ger även utbildningen till nyanställda eller inför att ett uppdrag påbörjas. Utbildningen innehåller följande delar:

- Hotbild
  Beskrivning av hotbilden med utgångspunkt från Livsmedelsverkets broschyr *Hotbilden mot dricksvatten och livsmedelsområdet.*
- Lagstiftning
  Genomgång av den lagstiftning som styr verksamhetens säkerhetsarbete.
- Säkerhetsskyddsanalys
  Beskrivning av hur arbetet med att ta fram verksamhetens säkerhetsskyddsanalys går till och hur den används inom verksamheten. Genomgång av de delar som är skyddsvärda i verksamheten – personal, anläggningar, information och försörjningsförmåga.
- Informationsklassning och sekretessbedömning
  Genomgång av vilka informationsklasser som används inom verksamheten och hur de tillämpas i praktiken. Beskrivning av arbetsgången vid sekretessbedömning i samband med utlämnande av allmän handling.
- Informationssäkerhet
  Beskrivning av verksamhetens interna riktlinjer för informationssäkerhet.
- Personalsäkerhet
  Beskrivning av verksamhetens interna riktlinjer för personalsäkerhet.
- Fysisk säkerhet
  Beskrivning av verksamhetens interna riktlinjer för fysisk säkerhet.

I utbildningen ingår också exempel på vad medarbetare och entreprenörer bör tänka på och känna till när de hanterar känslig information eller vid tillträde till verksamhetens anläggningar. Utbildningen tar också upp exempel på incidenter som har skett inom den egna verksamheten eller hos någon annan liknande verksamhet inom områdena informationssäkerhet, personalsäkerhet och fysisk säkerhet.

Systematiskt arbete med personalsäkerhet

Dricksvattenaktörer behöver hantera personalsäkerhetsfrågor på ett systematiskt sätt och integrera dem i den ordinarie verksamheten, på samma sätt som arbetet med informationssäkerhetsarbetet. Åtgärder krävs vid rekrytering, under anställningstiden och när en anställning upphör (se figur 4).



Figur 4. Exempel på åtgärder för ett systematiskt arbete med personalsäkerhet.

Dricksvattenaktörer som bedriver säkerhetskänslig verksamhet måste uppfylla särskilda krav på personalsäkerhet, se avsnittet *Personalsäkerhet inom ramarna för säkerhetsskyddslagstiftningen*.

Vid rekrytering

I samband med rekrytering av personal kan dricksvattenaktören genomföra ett antal åtgärder för att minska risken att anställa personal som skulle kunna utgöra en säkerhetsrisk:

- ställa säkerhetsrelaterade frågor vid anställningsintervjun
- göra en noggrann referenstagning
- ta alkohol- och drogtest
- genomföra bakgrundskontroller.

Dessa åtgärder syftar till att bedöma en persons lojalitet, pålitlighet och eventuella sårbarheter. Ekonomisk situation, familjesituation, missbruksproblematik och intressekonflikter kan vara områden som påverkar säkerhetsbedömningen.

Bilaga 3 innehåller exempel på frågor som kan ställas i samband med en säkerhets-bedömning vid nyanställning. Det är lämpligt att någon annan än den närmaste chefen genomför säkerhetsbedömningen, till exempel personal- eller säkerhetsavdelningen. Tänk på att de krav som ställs vid rekrytering och som avgör om en person kan få tjänsten eller inte ska anges i platsannonsen. Vissa av åtgärderna ovan kan också kräva kandidatens godkännande.

Under anställning

Tydliga riktlinjer och utbildning är två centrala delar i det löpande arbetet med personalsäkerhet. Det är viktigt att bygga en säkerhetskultur i verksamheten. Dricksvattenaktörer kan skapa förutsättningar för en säkerhetsmedveten organisation genom att låta all personal regelbundet genomgå en säkerhetsutbildning. Andra åtgärder innefattar bland annat:

- sekretessförbindelse för personal som har tillgång till sekretessreglerad information, se bilaga 4 för ett exempel
- regelbundna säkerhetssamtal, till exempel i samband med medarbetarsamtal
- rutiner för att fånga upp förändringar i den anställdes livssituation som skulle kunna påverka lojalitet och pålitlighet, skapa en personkännedom.

När en anställning ska upphöra

När en anställd avslutar sin anställning är det bra att hålla ett avslutande säkerhets-samtal. Ett bra avslut minskar risken för illojala handlingar mot verksamheten. Om medarbetaren tidigare har undertecknat en sekretessförbindelse är det också viktigt att påminna om att tystnadsplikten gäller även när anställningen upphört.

Det är viktigt att det finns rutiner för att exempelvis plocka bort behörigheter till system och anläggningar i samband med att en anställning upphör. Det är också viktigt att all dokumentation, nycklar, passerkort/taggar samt utrustning som telefon och dator återlämnas när anställningen upphör.

Extern personal

Det är inte enbart den egna personalen som kan behöva bedömas och utbildas ur ett säkerhetsperspektiv. Detsamma gäller extern personal från exempelvis konsultbolag och entreprenörer som har tillgång till sekretessreglerade uppgifter eller känsliga dricksvattenanläggningar. Det behövs en sekretessförbindelse om extern personal ska få tillgång till sekretessreglerade uppgifter, se bilaga 4 för exempel. Även besökare, praktikanter och personal som anlitas via frivilliga försvarsorganisationer kan omfattas av verksamhetens rutiner för personalsäkerhet.

Personalsäkerhet inom ramarna för säkerhets-skyddslagstiftningen

Personalsäkerhet är en del av säkerhetsskyddet för de verksamheter som omfattas av säkerhetsskyddslagstiftningen. Personalsäkerhet ska motverka att personer som inte är pålitliga ur säkerhetssynpunkt arbetar i säkerhetskänslig verksamhet. Personalsäkerhet ska även säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.[22]

Utbildning

Den som bedriver säkerhetskänslig verksamhet är skyldig att se till att berörd personal får utbildning i säkerhetsskydd. Utbildningen ska även följas upp regelbundet så länge personalen deltar i den säkerhetskänsliga verksamheten.[23]

Placering i säkerhetsklass

Dricksvattenaktören behöver genomföra en befattningsanalys utifrån säkerhetsskydds-analysen för att identifiera vilka befattningar som bör placeras i säkerhetsklass. Med befattningsanalysen som underlag fattas beslut om placering av en anställning eller ett uppdrag i säkerhetsklass. Det finns tre säkerhetsklasser (se tabell 3).

En anställning i staten, en kommun eller en region som är placerad i säkerhetsklass 1 eller 2 får endast innehas av den som är svensk medborgare.[24]

[22] 2 kap, 4 § säkerhetsskyddslagen (2018:585).

[23] 5 kap, 1 § säkerhetsskyddsförordningen (2021:955).

[24] 3 kap, 11 § säkerhetsskyddslagen (2018:585).

Tabell 3. Säkerhetsklasser och beslutsmandat för att besluta om placering i säkerhetsklass.

Säkerhetsklass	Beskrivning	Beslut om placering i säkerhetsklass[25]
1	I en omfattning som inte är ringa får del av uppgifter i säkerhetsskyddsklassen kvalificerat hemlig, eller som till följd av sitt deltagande i verksamheten har möjlighet att orsaka synnerligen allvarlig skada för Sveriges säkerhet.	Beslut om placering i säkerhetsklass 1 fattas av *regeringen* efter begäran från kommun, region eller myndighet.
2	Uppgifter i säkerhetsskyddsklassen *hemlig och kvalificerat hemlig (i ringa omfattning)* eller till följd av sitt deltagande i verksamheten har möjlighet att orsaka *allvarlig skada* för Sveriges säkerhet.	*Kommuner och kommunalförbund* kan fatta beslut om placering i säkerhetsklass 2 och 3 när det gäller anställning eller annat deltagande i den egna verksamheten. Kommunala bolag kan inte själva besluta om placering i säkerhetsklass 2 och 3, utan får gå genom sin ägarkommun[26]. Om bolaget ägs av flera kommuner behöver en överenskommelse göras om vilken av ägarkommunerna som fattar beslut om placering i säkerhetsklass.
3	Uppgifter i säkerhetsskyddsklassen *konfidentiell och hemlig (i ringa omfattning)* eller till följd av sitt deltagande i verksamheten har möjlighet att orsaka *skada som inte är obetydlig* för Sveriges säkerhet.	

[25] 5 kap, 5–10 § säkerhetsskyddsförordning (2021:955).

[26] Rättsligt bestämmande inflytande definieras i offentlighets- och sekretesslagen (2009:400), 2 kap. 3 §.

Exempel: Sandköping vatten och avfall AB genomför en befattningsanalys

En säkerhetsskyddsanalys har visat att delar av Sandköping vatten och avfalls verksamhet är säkerhetskänslig verksamhet inom ramen för säkerhetsskyddslagen (2018:585).

Befattningsanalys

Bolaget genomför därför en befattningsanalys utifrån säkerhetsskyddsanalysen. Det är en förteckning över vilka befattningar som deltar i den säkerhetskänsliga verksamheten och som bör placeras i säkerhetsklass. Analysen dokumenteras i en tabell. Befattnings-analysen omfattas av sekretess enligt 18 kap. 13 § OSL.

Befattning	Arbetsuppgifter	Tillgång till säkerhetsskydds-klassificerade uppgifter	Deltagande i övrig säkerhetskänslig verksamhet	Konsekvensnivå A–D (skada som befattningen kan orsaka för Sveriges säkerhet)	Föreslagen säkerhetsklass
VD	Leder verksamheten	Hemlig	Tillgång till anläggningar dagtid	B	2
Säkerhetschef	Leder och följer upp verksamhetens säkerhetsarbete	Hemlig	Obegränsad tillgång till alla anläggningar	B	2
Projektledare	Leder investerings-projekt	Konfidentiell	Tillgång till anläggningar dagtid	C	3
IT-tekniker	Ansvarar för drift och underhåll av IT-system	Konfidentiell	Tillgång endast till kontorslokaler	C	3
Driftpersonal	Ansvarar för drift och underhåll av anläggningar	Konfidentiell	Obegränsad tillgång till alla anläggningar	C	3
Ledningsnäts-personal	Ansvarar för drift och underhåll av ledningsnät	Konfidentiell	Obegränsad tillgång till alla anläggningar	C	3
Laboratorie-personal	Utför provtagning och analys	Begränsat hemlig	Tillgång till anläggningar dagtid	D	Säkerhets-prövning utan registerkontroll
Lokalvårdare	Utför lokalvård i verksamhetens kontorslokaler	Nej	Tillgång till kontorslokaler dagtid	-	-
…					

I nästa steg analyserar bolaget om de kan tillgodose behovet av säkerhetsskydd på något annat sätt än placering i säkerhetsklass. Det kan exempelvis vara åtgärder för att begränsa tillgången till viss information eller till vissa delar av anläggningen.

Begäran om placering i säkerhetsklass

Därefter skickas en begäran till ansvarig myndighet om att fatta beslut om placering av ett antal befattningar i säkerhetsklass. Ansvarig myndighet i detta fall är Sandköpings kommun, eftersom Sandköpings Vatten och Avfall som kommunalt bolag inte själva kan besluta om placering i säkerhetsklass.

Ansvar och tillsyn

Sandköpings vatten och avfall är en egen juridisk person och betraktas som enskild verksamhetsutövare. Det innebär också att VA-bolaget ansvarar för att den säkerhets-känsliga verksamheten bedrivs i enlighet med gällande lagstiftning och föreskrifter inom säkerhetsskydd. Tillsynsmyndighet är länsstyrelsen.

Säkerhetsprövning

Den som ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas.[27] Säkerhetsprövningen består av olika delar (se figur 5).

Figur 5. De olika stegen i en säkerhetsprövning. Registerkontroll och personutredning förutsätter att befattningen är placerad i säkerhetsklass.

Grundutredning

Det första steget i en säkerhetsprövning är att göra en utredning om personliga förhållanden som syftar till att skapa en personkännedom. Grundutredningen ska omfatta:[28]

- säkerhetsprövningsintervju
- inhämtning och bedömning av betyg, intyg och referenser
- identitetskontroll.

Säkerhetsprövningsintervjun ska pröva lojalitet, pålitlighet och sårbarhet hos person som prövas. Säkerhetspolisens vägledning *Personalsäkerhet* ger exempel på frågeområden som kan behandlas under samtalet, bland annat utbildning, tidigare anställningar, ekonomisk situation, familjesituation, fritidsintressen, vänner och personlig hälsa.[29] Se även bilaga 4 för förslag på frågor att ställa i samband med en säkerhetsprövningsintervju.

---

[27] 3 kap, 1 § säkerhetsskyddslagen (2018:585).

[28] 5 kap, 2 § säkerhetsskyddsförordningen (2021:955).

[29] Säkerhetspolisen (2023), *Personalsäkerhet*. https://sakerhetspolisen.se/download/18.3baf70bf187108c7cf04b8/1681802220657/Personalsäkerhet_anpassad.pdf.

Registerkontroll

En registerkontroll ska göras för personer som deltar i säkerhetskänslig verksamhet och som har en befattning som placerats i säkerhetsklass (se avsnitt *Placering i säkerhetsklass*). Registerkontrollen genomförs av Säkerhetspolisen efter ansökan från dricksvattenaktören. Om dricksvattenaktören är ett kommunalt bolag så är det ägarkommunen som gör ansökan. Ansökan ska göras efter att grundutredningen är genomförd och personen i fråga har bedömts som lojal och pålitlig ur ett säkerhetsskyddsperspektiv.

En registerkontroll innebär att Säkerhetspolisen undersöker om den som ska anställas eller på annat sätt ska delta i säkerhetskänslig verksamhet förekommer i till exempel belastningsregistret eller misstankeregistret. Om den kontrollerade personen förekommer i något av de register som kontrolleras är det Registerkontrolldelegationen som beslutar om uppgiften ska lämnas ut eller inte till den arbets- eller uppdragsgivare som har ansökt om kontrollen. Men det är alltid dricksvattenaktören själv som fattar beslutet om anställning. Registerkontrolldelegationen är en del av Säkerhets- och integritetskyddsnämnden, www.sakint.se.

Den som registerkontrolleras ska lämna sitt samtycke till att registerkontrollen utförs och det är dricksvattenaktören som ansvarar för att dokumentera samtycket.[30] Vid registerkontroll i säkerhetsklass 1 och 2 kontrolleras även make, maka eller sambo. Dessa behöver inte lämna samtycke till att registerkontrollen utförs.

Det ska göras en ny registerkontroll om en person byter befattning hos verksamhetsutövaren. Det är också viktigt ur integritetssynpunkt att registerkontrollen avslutas när personen ifråga har avslutat sin anställning eller sitt uppdrag. När anställningen eller uppdraget upphör, ska det därför anmälas till Säkerhetspolisen.

Särskild personutredning

För befattningar som har placerats i säkerhetsklass 1 och 2 ska även en särskild personutredning genomföras[31], utöver grundutredning och registerkontroll. Den särskilda personutredningen innefattar en kontroll av den berördes ekonomiska förhållanden och genomförs av Säkerhetspolisen.

[30] 3 kap, 18 § säkerhetsskyddslagen (2018:585) och 5 kap, 15 § säkerhetsskyddsförordningen (2021:955).

[31] 3 kap, 17 § säkerhetsskyddslagen (2018:585).

Extern personal i säkerhetskänslig verksamhet

Kraven på säkerhetsskydd är samma oavsett om den säkerhetskänsliga verksamheten bedrivs med hjälp av egen eller extern personal. När konsulter och underleverantörer anlitas kan dricksvattenaktören därför behöva teckna ett säkerhetsskyddsavtal eller en säkerhetsskyddsöverenskommelse med dem. Det innebär att leverantören har ansvar för att uppfylla säkerhetsskyddskraven, bland annat inom området personalsäkerhet. Dricksvattenaktören har ansvar att kontrollera att villkoren i avtalet eller överenskommelsen följs. Läs mer i avsnittet *Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)* och i Säkerhetspolisens vägledning *Skyldigheter vid exponering av säkerhetskänslig verksamhet.*[32]

Fördjupning: Vill du läsa mer?

Svenskt Vatten (2023) Säkerhetshandbok för dricksvattenproducenter P118 https://vattenbokhandeln.svensktvatten.se/produkt/sakerhetshandbok-for-va-verksamhet-digital-version/.

Säkerhetspolisen har flera vägledningar inom säkerhetsskydd. Stora delar av innehållet kan vara användbart för verksamheter som inte omfattas av säkerhetsskyddslagen. https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html.

[32] Säkerhetspolisen (2023), *Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet* https://sakerhetspolisen.se/download/18.3222e1b7187a064b070e6/1683815514604/Skyldighet%20vid%20exponering%20av%20sa%CC%88kerhetska%CC%88nslig%20verksamhet_anpassad.pdf.

Fysisk säkerhet

I en dricksvattenverksamhet utgör fysisk säkerhet en stor del av säkerhetsarbetet. Åtgärder inom fysisk säkerhet syftar till att

- förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt
- förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt
- skydda mot att obehöriga får insyn i verksamheten, med eller utan tekniska hjälpmedel som till exempel drönare.

Fysisk säkerhet är en kombination av rutiner, byggnads- och säkerhetsteknik för att skydda områden och anläggningar. Skyddsåtgärder kan bestå av såväl fysiska som administrativa åtgärder.

Fysiska skyddsåtgärder kan till exempel innefatta bevakningspersonal, lås och larm, bevakningssystem och stängsel. En dokumenterad strategi för hur det fysiska skyddet (områdesskydd, skalskydd) och det tekniska skyddet (larm och bevakning) utformas för dricksvattenanläggningarna underlättar säkerhetsarbetet. Strategin kan vara i form av tekniska anvisningar eller projekteringsanvisningar som tillämpas vid alla ny- och ombyggnationer. Utgångspunkten för sådana anvisningar anpassas efter anläggningens skyddsbehov och hur kritisk den är för verksamheten. Det är inte säkert att alla dricksvattenanläggningar behöver samma typ av skydd. Tänk på att även kontors-byggnader kan behöva skyddas.

Administrativa skyddsåtgärder kan bland annat inkludera rutiner för vilka som får tillträde till anläggningar och rutiner för in- och utpassering för såväl egen personal som entreprenörer och besökare, se exempel i bilaga 5. Det är också viktigt att det finns rutiner för hur larm hanteras, exempelvis brandlarm, inbrottslarm och områdes-bevakningslarm. Ett larm är verkningslöst om det inte finns rutiner för hur personalen ska agera för att hantera larmet.

Vattenverk, reservoarer och tryckstegringsstationer är exempel på områden och anläggningar som behöver skyddas. Ett svagt fysiskt skydd ökar risken för till exempel inbrott, sabotage eller brand. Det kan få allvarliga och kostsamma konsekvenser för dricksvattenförsörjningen.

Exempel: Sandköping vatten och avfall AB:s tekniska anvisningar för fysisk och teknisk säkerhet

Sandköping vatten och avfall har tagit fram tekniska anvisningar för fysisk och teknisk säkerhet. Anvisningarna används vid projektering av nya anläggningar. De är också en del i bolagets säkerhetsskyddsplan eftersom en åtgärd i planen är att anpassa befintliga byggnader för att möta kraven i de tekniska anvisningarna.

Utgångspunkt för omslutningsytor i anläggningar och särskilda utrymmen är skyddsklass enligt SSF200, och för områdesskydd klass/risknivå enligt SSF1087. För arkivlokaler gäller även Riksarkivets föreskrifter RA-FS. Sandköping Vatten och avfall har bland annat kategoriserat sina anläggningar baserat på en bedömning av hur kritiska de är för att upprätthålla dricksvatten-försörjningen, antalet personer de försörjer och hur omgivningen ser ut där de är placerade. Bolaget har landat i följande klassning:

Anläggning	Yttre omslutningsyta Skyddsklass enligt SSF200	Områdesskydd Klass/Risknivå enligt SSF1087
Vattenverk	SK3	C3
Högreservoar	SK3	C2
Tryckstegringsstation	SK2	C2
Ventilkammare	SK2	-
Kontorsbyggnad	SK2	-

Särskilda utrymmen	Inre omslutningsyta Skyddsklass enligt SSF200
Driftrum	SK2
Processrum	SK2
Elrum	SK2
Serverrum	SK3
Arkiv	SK2

Motsvarande genomgång och kategorisering har gjorts även för inbrottslarm. Utgångspunkt är larmklass enligt SSF100. Bolaget har landat i följande klassning:

Anläggning	Yttre omslutningsyta Larmklass enligt SSF100	Övrigt
Vattenverk	LK2	Särskilda utrymmen med egen larmklass förekommer
Högreservoar	LK2	
Tryckstegringsstation	LK2	
Ventilkammare	-	Endast dörrlarm anslutet till styrsystem
Kontorsbyggnad	LK2	Särskilda utrymmen med egen larmklass förekommer

Särskilda utrymmen med egen larmklass	Inre omslutningsyta Skyddsklass enligt SSF200
Driftrum	LK2
Processrum	LK2
Elrum	LK2
Serverrum	LK3
Arkiv	LK3

Motsvarande bedömningar har gjorts även för brandlarmsystem, områdeslarmsystem, passerkontrollsystem, porttelefonisystem och tv-övervakningssystem. Alla avsteg från och tillägg till de grundläggande kravnivåerna beskrivs detaljerat i de tekniska anvisningarna.

Systematiskt arbete med fysisk säkerhet

Det viktigt att arbetet med den fysiska säkerheten bedrivs kontinuerligt och systematiskt för att upprätthålla säkerheten. De fyra stegen nedan beskriver ett exempel på en arbetsgång som kan tillämpas och som innefattar analys av behov, utformning, kontroll och justering av åtgärder. Det är viktigt att dricksvattenaktören aktivt förvaltar säkerhetssystemen med all tillhörande administration, åtgärder och kontroller.

Steg 1. Analys

Det första steget i ett systematiskt arbete med fysisk säkerhet är att beskriva nuläget:

- Hot och sårbarheter? Konsekvenser vid eventuellt sabotage eller skadegörelse?
- Vilka anläggningar, byggnader och områden behöver skyddas?
- Vilken säkerhetsnivå finns i dag?
- Vilka är behöriga att få tillträde till de skyddsvärda anläggningarna?
- Vilka krav gäller för den fysiska säkerheten (lagar, föreskrifter, interna riktlinjer)?

Steg 2. Utformning

Geografiskt läge, byggnadstekniska förutsättningar och verksamhetens/anläggningens betydelse för dricksvattenproduktionen påverkar utformningen av den fysiska säkerheten.

Steg 3. Kontroll och utvärdering

- Kontrollera larm och bevakningssystem.
- Kontrollera stängsel, lås och bommar.
- Öva och utvärdera hanteringen av ett olovligt intrång på en anläggning.
- Sammanställ statistik och utvärdera alla säkerhetsincidenter, inklusive skadegörelse.

Steg 4. Eventuella justeringar såsom att

- införa tätare ronderingar
- införa rutin för ledsagning av besökare
- flytta kamerabevakning till platser som oftare utsätts för skadegörelse.

Åtgärder för att upptäcka, försvåra och hantera

I arbetet med fysisk säkerhet krävs ofta en kombination av åtgärder för att upptäcka, försvåra och hantera exempelvis intrång och sabotage. Exempel på åtgärder inom respektive område beskrivs i tabell 4.

Tabell 4. Åtgärder för att upptäcka, försvåra och hantera exempelvis intrång och sabotage.

Metod	Åtgärd
Upptäcka	inbrottslarm
	kamerabevakning
	ronderingar
	områdeslarm, till exempel markradar
	brandlarm
Försvåra	områdesskydd (stängsel, grindar, bommar)
	skalskydd (omslutningsyta inklusive lås, dörrar, fönstergaller etcetera)
	rutiner för nycklar och taggar
	passersystem
	rutiner för in- och utpassage av personal, entreprenörer, konsulter, gods/leveranser
Hantera	rutiner för att hantera larm, till exempel utryckning av väktare
	rutiner för polisanmälan och rapportering till Säkerhetspolisen
	rutiner för att upptäcka och åtgärda fel och brister

Flera av åtgärderna för att upptäcka och försvåra kan också ha en avskräckande effekt. Det vill säga att den som planerar att begå ett inbrott eller genomföra ett sabotage undviker det på grund av risken för att bli upptäckt. Andra exempel på avskräckande åtgärder kan vara att ha områdesbelysning eller närvarostyrd belysning vid dricksvattenanläggningar.

Ytterligare exempel på åtgärder för att minska risken för inbrott eller stöld kan vara att hålla stöldbegärlig utrustning borta från fönster eller inlåst även när den förvaras i låsta byggnader. Stöldmärkning av utrustning och GPS-spårning av utrustning, till exempel fordon, kan också vara effektiva åtgärder för att minska risken för stöld, om det framgår att utrustningen skyddas på det sättet.

Exempel: Säkerhetsåtgärder hos Sandköping vatten och avfall AB

Sandköping vatten och avfall har haft flera säkerhetsrelaterade händelser i och vid sina anläggningar. Därför har de vidtagit extra säkerhetsåtgärder som en del i det kontinuerliga arbetet med att förbättra säkerheten.

- Efter flera incidenter där en tryckstegringsstation blev påkörd av fordon har de satt upp påkörningsskydd i form av så kallade pollare som skyddar fasaden.
- Efter ett misstänkt sabotageförsök i en av grundvattenbrunnarna har de kompletterat skyddet och larmsystemet på alla brunnar så att det vid åverkan på skyddshuven först går ett tyst larm till driftcentralen samtidigt som pumpen stannar. Vid åverkan även på skyddsluckan utlöses ett akustiskt larm på platsen.
- För att undvika risk för att någon med uppsåt eller av misstag ”smittar” det industriella informations- och styrsystemet med virus har de fysiskt blockerat alla USB-portar och nätverksportar. Vid behov kan dessa låsas upp av den egna personalen som då övervakar åtgärden.
- Efter upprepade fall av klotter på en anläggning monterades stängsel runt anläggningen. Eftersom möjligheten fanns stängslades ett större område in vilket skapar ett extra avstånd från allmän yta till anläggningen, vilket även försvårar möjligheten att störa ut anläggningens OT-system.
- Efter flera fall av sönderklippta hänglås till ventilkammarluckor har larm installerats som ger en signal till driftcentralen när luckorna öppnas.
- På grund av problem med personer som försöker smita in på anläggningen genom att följa efter med sin bil när körgrinden öppnas har grinden bytts ut mot en singelpassagegrind. Grinden är dessutom av viktyp och öppnar och stänger på bara några sekunder. Det går ett larm till driftcentralen om någon försöker smita in och fastnar i grinden, det vill säga om grindens klämskydd aktiveras. Sandköping vatten och avfall har haft flera säkerhetsrelaterade händelser i och vid sina anläggningar. Därför har de vidtagit extra säkerhetsåtgärder som en del i det kontinuerliga arbetet med att förbättra säkerheten.

Skyddsobjekt

Enligt 4 § i skyddslagen (2010:305) kan länsstyrelsen besluta att byggnader, andra anläggningar och områden som har betydelse för Sveriges försörjningsberedskap ska vara skyddsobjekt. För dricksvattenförsörjning kan det exempelvis vara vattenverk, reservoarer, tryckstegringsstationer, synliga brunnskonstruktioner, infiltrations-bassänger, infiltrationsytor, pumphus, processdelar, vattenreservoarer, mindre vattentäkter och infrastruktur tillhörande reservvattentäkter.

Det finns flera fördelar med att ansöka om och få ett beslut om skyddsobjekt. Några exempel är att:

- obehöriga förbjuds tillträde till objektet och kan avvisas
- det inte krävs tillstånd för kamerabevakning
- kamerabevakning inte behöver skyltas
- skyddsvakter (som har utökade befogenheter jämfört med väktare) kan användas för bevakningsåtgärder och för insatser.

Vid ansökan om skyddsobjekt är det också möjligt att ansöka om förbud mot att göra avbildningar, beskrivningar och mätningar av eller inom skyddsobjektet (fotoförbud).

Ansökan om skyddsobjekt görs av dricksvattenaktören och kräver medgivande från fastighetsägaren. Länsstyrelsen fattar beslut om skyddsobjekt. I ansökan behöver det framgå vilken skyddsvärd verksamhet som sker och vilken hotbild som finns mot verksamheten. Det är aktören själv som ansvarar för skyddet av skyddsobjektet.

Hot och våld mot personal

Arbetet inom fysisk säkerhet kan även kopplas till arbetsgivarens ansvar enligt Arbetsmiljöverkets föreskrift (AFS 1993:2) att utreda och åtgärda eventuella risker för hot och våld mot personal.[33] Föreskrifterna tar bland annat upp ensamarbete, säkerhetsrutiner samt utbildning och övning i att hantera olika situationer, till exempel vid larm. Detta område beskrivs inte närmare i denna handbok.

Fysisk säkerhet inom ramarna för lås och bom-föreskriften

Dricksvattenaktörer som omfattas av lås och bom-föreskriften måste uppfylla krav på åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar. Åtgärderna syftar till att förebygga och avhjälpa skadeverkningar genom att:

- säkerställa att obehöriga personer inte kan bereda sig tillträde till vattenverk
- obehöriga personer inte kan bereda sig tillträde till hög- och lågreservoarer, tryckstegringsstationer och liknande anläggningar
- övriga delar av distributionsanläggningen skyddas mot obehörig åtkomst.

Enligt föreskrifterna ska berörda producenter och distributörer upprätta en handlingsplan för hur de kan upptäcka sabotage och annan skadegörelse riktad mot vattenverk och distributionsanläggningar och hur de kan avhjälpa skadeverkningarna.

Fysisk säkerhet inom ramarna för säkerhetsskyddslagstiftningen

Verksamheter som omfattas av säkerhetsskyddslagen måste uppfylla särskilda krav på fysisk säkerhet. Det gäller områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter förvaras eller annars behandlas, eller där säkerhetskänslig verksamhet i övrigt bedrivs. Dessa ska vara försedda med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan utifrån ett

[33] Arbetsmiljöverkets föreskrift (AFS 1993:2). *Våld och hot i arbetsmiljön.* Våld och hot i arbetsmiljön (AFS 1993:2), föreskrifter – Arbetsmiljöverket (av.se).

identifierat säkerhetsskyddsbehov.[34] Mer om detta finns att läsa i Säkerhetspolisens *Vägledning i säkerhetsskydd – Fysisk Säkerhet*.

Fördjupning: Vill du läsa mer?

Livsmedelsverkets kontrollwiki om lås och bom-föreskriften LIVSFS 2008:13 Åtgärder mot sabotage och annan skadegörelse – Kontrollwiki (livsmedelsverket.se).

Svenskt Vatten (2023). *Säkerhetshandbok för dricksvattenproducenter P118* https://vattenbokhandeln.svensktvatten.se/produkt/sakerhetshandbok-for-va-verksamhet-digital-version/.

Säkerhetspolisen har flera vägledningar inom säkerhetsskydd. Stora delar av innehållet är även relevant för verksamheter som inte omfattas av säkerhetsskyddslagen. https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html.

Svenska kraftnät har tekniska riktlinjer kopplat till fysiskt skydd som även är användbara för dricksvattenanläggningar, TR09-serien. https://www.svk.se/aktorsportalen/entreprenorer-i-elnatet/tekniska-riktlinjer/.

[34] 4 kap, 1 § säkerhetsskyddsförordningen (2021:955).

Upphandling

Den verksamhet som dricksvattenaktörer bedriver innebär att det ofta finns behov av att skydda sekretessreglerade uppgifter i samband med upphandling. Det är alltid dricksvattenaktörens ansvar att skydda dessa uppgifter. Ett vanligt sätt att skydda sekretessreglerade uppgifter i samband med en upphandling är att upprätta sekretess- och säkerhetsavtal med anbudsgivare, se avsnitt *Upphandling med sekretess- och säkerhetsavtal*. I de fall det gäller säkerhetsskyddsklassificerade uppgifter ska upphandlingen ske enligt säkerhetsskyddslagstiftningen, se avsnitt *Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)*. Notera att om anbudsgivaren kan få tillgång till uppgifter med säkerhetsskyddsklass konfidentiell eller högre, eller tillgång till säkerhetskänslig verksamhet av motsvarande betydelse, ställs krav på en särskild säkerhetsskyddsbedömning och lämplighetsprövning.[35]

Upphandling med sekretess- och säkerhetsavtal

Ibland kan anbudsgivare behöva få tillgång till sekretessreglerad information i samband med en upphandling. Ett sätt att hantera detta är att teckna sekretess- och säkerhetsavtal i ett tidigt skede under upphandlingen innan någon sekretessreglerad information delges anbudsgivarna. När upphandlingen är genomförd och uppdraget tilldelats sägs sekretess- och säkerhetsavtalet upp med de anbudsgivare som inte har fått uppdraget.

[35] 4 kap 8 § säkerhetsskyddslagen (2018:585).

Exempel: Upphandlingsprocess hos Sandköping vatten och avfall AB för att skydda sekretessreglerad information

Sandköping vatten och avfall har utvecklat en egen metod för upphandlingar där det förekommer sekretessreglerad information. De kallar metoden selektiv upphandling med sekretess- och säkerhetsavtal (SUSA). Det selektiva förfarandet innebär att de skriver sekretess- och säkerhetsavtal med alla anbudsgivare innan de får ta del av sekretess-reglerade uppgifter i upphandlingen, som till exempel ritningar eller andra underlag.

Arbetsmetoden innefattar flera steg:

1. Riskbedömning av upphandlingen. Upphandlingen ska genomföras som en SUSA om förfrågningsunderlaget innehåller uppgifter som är sekretessreglerade. Riskbedömningen ska också ta hänsyn till hur anbuden från entreprenören ska lämnas.
2. Beslut om selektivt förfarande. Projektledaren eller ansvarig för upphandlingen beslutar om att genomföra upphandlingen som en SUSA innan annonsering. Det är rekommenderat att samråda med säkerhetsansvarig och upphandlingsansvarig innan upphandlingen publiceras.
3. Leverantören ansöker om att få lämna anbud.
4. Sekretess- och säkerhetsavtal tecknas med samtliga anbudsgivare som ska få ta del av handlingarna.
5. Handlingarna skickas till anbudslämnaren på ett säkert sätt.
6. Leverantören lämnar anbud.
7. Utvärdering av anbud och tilldelning av vinnande anbud.
8. Handlingarna återtas från de som inte vunnit upphandlingen. Ta hänsyn till eventuell överprövning.
9. Uppsägning av sekretess- och säkerhetsavtal med de som inte har vunnit upphandlingen. Påminnelse om att de fortfarande är bundna av tystnadsplikt.

Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)

Intressen vars säkerhet regleras av säkerhetsskyddslagstiftningen ska ha samma nivå av säkerhet oavsett om de hanteras av verksamhet som bedrivs av offentliga eller privata aktörer. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) är en följd av den principen. Säkerhetsskyddad upphandling är en process som i huvudsak går ut på att

- identifiera berörda skyddsvärden i en upphandling
- analysera skyddsvärden
- ta fram ett säkerhetsskyddsavtal.

Dricksvattenaktörer är bara skyldiga att ingå säkerhetsskyddsavtal när det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskydds-klassen konfidentiell eller högre. Det gäller även när leverantören får tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Sådan verksamhet kan ha ett högt skyddsvärde trots att den inte rör säkerhetsskydds-klassificerade uppgifter, exempelvis:[36]

- verksamhet vid kärnkraftverk, flygplatser eller dricksvattenverksamhet som bedrivs vid skyddsobjekt enligt *skyddslagen (2010:305)*
- digital infrastruktur eller system för styrning och övervakning av kritiska processer i dricksvattenförsörjningen
- handlingar och informationssystem med ett betydande skyddsvärde utan att de innehåller säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddsavtalet utgör också en grund för att besluta om vilka anställningar och annat deltagande hos motparten som ska placeras i säkerhetsklass. Läs mer under avsnitt *Placering i säkerhetsklass*.

Ett säkerhetsskyddsavtal binder leverantören till att uppfylla de ställda säkerhetsskydds-kraven. Den dricksvattenaktör som ingår säkerhetsskyddsavtalet är ansvarig för att löpande kontrollera att bestämmelserna i avtalet uppfylls.

Tänk på att en dricksvattenaktör som planerar att ingå ett säkerhetsskyddsavtal ska anmäla det till tillsynsmyndigheten, det vill säga Länsstyrelsen i Skåne, Västra Götaland, Stockholm eller Norrbotten. I vissa fall ska även samråd ske innan avtal

[36] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet*, 2023.

tecknas. Dricksvattenaktören ska även meddela tillsynsmyndigheten när ett säkerhetsskyddsavtal upphör, eller om avtalet förlängs utöver den sluttid som tidigare har angetts. För närmare information om säkerhetsskyddad upphandling, se Säkerhetspolisens vägledning *Skyldigheter vid exponering av säkerhetskänslig verksamhet*.

Säkerhetsskyddsöverenskommelse

Det är dricksvattenaktörens skyldighet att se till att uppgifter i en upphandling har nödvändigt skydd även om det i en upphandling gäller säkerhetsskyddsklassificerade uppgifter i säkerhetsklass begränsat hemlig (eller få tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet) då lagstiftningen inte ställer krav på säkerhetsskyddsavtal.[37] Det går att åstadkomma det nödvändiga skyddet genom att tillämpa en liknande process som vid säkerhetsskyddad upphandling med säkerhetsskyddsavtal. Skillnaden är att befattningar hos motparten inte placeras i säkerhetsklass och att säkerhetsskyddsavtalet ersätts med en säkerhetsskyddsöverenskommelse som reglerar vilka krav dricksvattenaktören ställer på motparten.

[37] 7 kap. 11 § Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2022:1.

Bilaga 1. Stöd vid sekretess-bedömning och utlämnande av allmän handling

Den här bilagan innehåller ett stöd till dricksvattenaktörer vid sekretessbedömning och utlämnande av allmän handling.

Offentlighet och sekretess

Offentlighetsprincipen

Offentlighetsprincipen är en grund för vår demokrati.[38] Offentlighetsprincipen är också en garant för rättssäkerhet och effektiv offentlig förvaltning. Enligt offentlighets-principen ska vem som helst, när som helst, kunna få se eller få en kopia av en allmän handling hos en myndighet eller till exempel ett kommunalt bolag eller ett kommunal-förbund.

Vad är en allmän handling?

En allmän handling[39] är en handling som förvaras[40] och som har skickats till[41] eller upprättats på en myndighet. De flesta handlingar som finns hos en myndighet är allmänna handlingar. Ett utkast som tas fram inför ett beslut eller ett underlag för korrektur[42] är exempel på handlingar som normalt sett *inte* är allmänna. Dessa behöver alltså inte lämnas ut om någon frågar efter dem.

Länkar

Tryckfrihetsförordningen (1949:105)

[38] Regeringsformen (1974:152), Tryckfrihetsförordningen (1949:105).

[39] 2 kap. 4 § TF.

[40] 2 kap. 6 § TF.

[41] 2 kap. 9 § TF.

[42] 2 kap. 12 § TF.

En allmän handling ska lämnas ut genast eller skyndsamt

En person som vill komma till myndigheten och ta del av en allmän handling på plats har rätt att göra det genast eller så snart det är möjligt.[43] Alla har också rätt att ta del av kopior av allmänna handlingar. Men det finns inga krav på att myndigheten ska lämna något annat än en papperskopia.[44] En fråga om att få en kopia av en allmän handling ska behandlas skyndsamt.[45] Svar på frågan om att få ta del av en handling bör normalt lämnas samma dag som frågan ställdes.[46] Om myndigheten behöver göra en sekretessbedömning kan beskedet lämnas efter någon eller några dagar. Huvudregeln är att det är den person på myndigheten som har ansvar för handlingen som är den som ska pröva om handlingen ska lämnas ut.[47] Om du är osäker på vem som ska pröva utlämningsärendet kan du titta i din organisations arbets- eller delegationsordning.

Länkar

Tryckfrihetsförordningen (1949:105)

Riksdagens ombudsmän (JO)

Sekretess

Det finns vissa uppgifter i allmänna handlingar som inte alla bör kunna ta del av. Enligt grundlagen ska man ibland begränsa rätten att ta del av allmänna handlingar. En sådan begränsning måste anges noga i en särskild lag.[48] Den lagen är här *offentlighets- och sekretesslagen*, ofta förkortad OSL.

Om en uppgift i en allmän handling är sekretessbelagd får just den uppgiften i handlingen inte lämnas ut om någon frågar och den får heller inte publiceras. Den uppgiften får inte lämna organisationen, alltså inte **röjas**. Men eftersom handlingen är allmän ska resten av den lämnas ut vid förfrågan. Därför måste uppgiften som är sekretessbelagd döljas innan handlingen lämnas ut eller publiceras. På så sätt har offentlighetsprincipen och lagstiftningen följts. De uppgifter som alla har rätt att ta del av har lämnats ut, samtidigt som de uppgifter som de inte får ta del av har skyddats genom överstrykning.

---

[43] 2 kap.15 § TF.

[44] Se till exempel JO 733-12.

[45] 2 kap. 16 § TF.

[46] Se till exempel JO 2003/04 s. 389.

[47] 6 kap. 3 § OSL.

[48] 2 kap. 2 § TF.

Länkar

Tryckfrihetsförordningen (1949:105).

Offentlighets- och sekretesslagen (2009:400).

Den som begär ut en handling har rätt att vara anonym

Vi har alla rätt att ta del av allmänna handlingar utan att behöva uppge vilka vi är eller varför vi vill ta del av handlingen. När någon begär att få ta del av en allmän handling får du alltså inte fråga vem personen är eller varför den vill ta del av handlingen.[49]

När sedan sekretessbedömningen görs kan du däremot få fråga efter personens identitet och varför personen vill ta del av handlingen. Det får du göra i de fall du har kommit fram till att det finns uppgifter i handlingen som omfattas av sekretess, men det finns också omständigheter där vissa ändå har rätt att ta del av uppgifterna. Då spelar det roll vem det är som har gjort begäran. Vill inte personen uppge vem den är eller varför den vill ta del av handlingen, så att du kan avgöra om personen är behörig att se handlingen, får personen ta del av handlingen med de sekretessbelagda uppgifterna överstrukna. Läs mer i avsnittet *Sekretessbedömning mellan myndigheter*.

Länkar

Tryckfrihetsförordningen (1949:105).

Riksdagens ombudsmän (JO).

Delning mellan myndigheter

När en myndighet vill ha uppgifter från en annan myndighet gäller inte samma regler som när en privatperson, journalist, företag eller annan enskild frågar efter dem.

Uppgiften behöver inte vara en del av en allmän handling

Mellan myndigheter finns en informationsskyldighet.[50] I begreppet myndighet ingår till exempel också kommunala bolag och kommunalförbund. Enligt informations-skyldigheten ska en myndighet lämna ut en uppgift som en annan myndighet frågar efter, om inte uppgiften är sekretessbelagd eller om det skulle hindra arbetets behöriga gång. Att något hindrar arbetets behöriga gång skulle till exempel kunna vara att myndighetens uppdrag störs allvarligt om begäran skulle besvaras. Det räcker alltså inte att begäran omfattar många uppgifter eller tar tid från annat arbete. Om myndigheten har tillgång till uppgifterna eller kan sammanställa dem ska de lämnas ut. Det innebär

[49] 2 kap. 18 § TF och till exempel JO 2018/19 s. 320.

[50] 6 kap. 5 § OSL.

att en myndighet i regel har rätt att ta del av andra myndigheters uppgifter, även om uppgifterna inte är en del av en allmän handling. Myndigheter har alltså rätt att ta del av fler uppgifter hos varandra än allmänheten har.

Uppgiften måste inte alltid lämnas lika skyndsamt som till allmänheten

Justitieombudsmannen (JO) har sagt att utgångspunkten vid utlämnande av uppgifter till en annan myndighet är att prövningen ska göras med skyndsamhet.[51] Skyndsamt innebär att svar normalt bör lämnas samma dag som frågan kom till myndigheten.[52] Om myndigheten behöver göra en sekretessbedömning kan beskedet lämnas efter någon eller några dagar. Men vid utlämnanden mellan myndigheter menar JO att det bör finnas förhållandevis stort utrymme att beakta omständigheterna i det enskilda fallet. Myndigheten som frågar efter uppgiften kan till exempel ange en tid för när de vill ha den och då är det den tiden som den utlämnande myndigheten kan förhålla sig till. Det innebär att den utlämnande myndigheten inte måste lämna ut uppgifterna samma dag som frågan inkommer om den begärande myndigheten har angett en annan tid.

Sekretessbedömning mellan myndigheter

En uppgift hos en myndighet måste lämnas ut vid fråga från annan myndighet förutsatt att uppgiften inte är sekretessbelagd.[53] För att veta om uppgiften ska lämnas ut eller inte måste du alltså veta om den är sekretessbelagd.

Att en uppgift är sekretessbelagd innebär inte bara att det finns en bestämmelse i *offentlighets- och sekretesslagen* som ska användas. Dessutom måste du kunna anta att det skulle orsaka skada att lämna ut uppgiften just till den myndighet som har begärt ut den. Det finns sekretessbestämmelser som i huvudsak rör krisberedskap och totalförsvar som ska tillämpas av alla myndigheter. Bestämmelserna har konstruerats på ett sätt som gör att skyddsvärda uppgifter skyddas genom sekretess oavsett hos vilken myndighet de befinner sig. Eftersom sekretessbestämmelsen gäller även hos den myndighet som frågar efter uppgiften kan du i din sekretessbedömning anta att uppgiften har samma skydd hos den frågande myndigheten som hos din myndighet.[54] Därför är inte uppgiften sekretessbelagd i förhållande till en annan myndighet och ska lämnas ut.

---

[51] JO:s beslut dnr 9586-2020.

[52] Se till exempel JO 2003/04 s. 389.

[53] 6 kap. 5 § OSL.

[54] Prop. 2003/04:93 s. 82 f., prop. 2004/05:5 s.264., och HFD mål nr 1208–1210-21 dom meddelad 2021-12-22.

Tips!

Ibland frågar andra myndigheter efter uppgifter som du bedömer omfattas av sekretess. Du kan alltid skicka med ett följebrev när du lämnar ut uppgiften. I det kan du förklara hur du ser på uppgiftens skyddsvärde och vilken skada som skulle kunna uppstå om den röjdes. På så vis kan du underlätta för den andra myndigheten om uppgiften skulle begäras ut från dem och de måste göra en egen sekretessbedömning.

Du kan också skriva att myndigheten gärna får kontakta er om uppgiften begärs ut från dem. Då kan ni hjälpa dem med information till deras sekretessbedömning. Men tänk på att det alltid är den myndighet som får frågan om att lämna ut en allmän handling som ska göra sekretessbedömningen. Lika lite som du måste följa någon annan i din sekretessbedömning måste de följa dig i sin bedömning.

Aggregering av uppgifter

Ibland samlar myndigheter in uppgifter från andra. Uppgifterna kan ha ett lågt skyddsvärde, eller inget skyddsvärde alls, när de är utspridda en och en hos olika organisationer. Men i och med att de samlas, aggregeras, hos en myndighet kan sammanställningen få ett högre skyddsvärde. Det kan gälla uppgifter som från början inte ens omfattas av sekretess, men som i sammanställd form kommer att omfattas av sekretess om någon frågar efter dem. Det kan också gälla uppgifter som hos de enskilda organisationerna redan omfattas av sekretess och som när de sammanställs blir så skyddsvärda att de kan användas för att skada Sveriges säkerhet. Då krävs ett ännu starkare skydd och de omfattas då av ytterligare en lagstiftning, *säkerhetsskyddslagen*[55].

Den myndighet som frågar efter uppgifterna ska pröva om de omfattas av säkerhetsskydd. Om de omfattas av säkerhetsskydd ska myndigheten hantera dem i enlighet med säkerhetsskyddslagstiftningen. Om de inte omfattas av säkerhetsskydd ska myndigheten göra en sekretessbedömning av dem först om någon frågar efter dem.

Om flera eller alla uppgifter begärs ut på samma gång kan myndigheten som har samlat in uppgifterna under vissa förutsättningar sekretessbelägga dem även om uppgifterna inte är sekretessbelagda var för sig. Om myndigheten har bearbetat dem på ett sätt som tillför information, till exempel genom en analys, kan uppgifter behöva sekretessbeläggas. Myndigheten kan också sekretessbelägga uppgifterna om de tillsammans ger ny information som uppgifterna inte skulle ha avslöjat en och en. Ett exempel kan vara en försörjningskedja, där de olika uppgifterna om till exempel aktörer, produkter och

[55] Säkerhetsskyddslagen (2018:585).

volymer inte var för sig är skyddsvärda, men där bilden över hela kedjan kan ge information om förmågor och sårbarheter.

Däremot har en myndighet ingen möjlighet att sekretessbelägga uppgifterna om de begärs ut en och en. Inte heller finns det stöd att sekretessbelägga dem om flera eller alla uppgifter begärs ut samtidigt och de inte tillsammans utgör sådan information som omfattas av en sekretessbestämmelse.

Ibland får myndigheter begäran om allmänna handlingar som till exempel skulle kunna vara försök att kartlägga samhällsviktig verksamhet i Sverige. Det kan gälla sådan insamlad information som myndigheten har fått från andra aktörer. Myndigheten kan dock enbart sekretessbelägga uppgifter och sammanställningar som faktiskt omfattas av en sekretessbestämmelse. Om det finns en misstanke om att uppgifterna som finns i de begärda handlingarna ska användas i brottslig verksamhet får det meddelas den myndighet som ansvarar för att utreda och lagföra sådana brott. Om det gäller Sveriges säkerhet bör Säkerhetspolisen kontaktas och de får i sin tur får utreda om befattningen med uppgifterna är av sådan art att ett brott kan ha begåtts.

Sekretessbedömning

Vilken eller vilka bestämmelser i offentlighets- och sekretesslagen är tillämpliga?

För att en uppgift ska vara sekretessreglerad måste det finnas en bestämmelse i *offentlighets- och sekretesslagen* som gäller för uppgiften.[56] Det första du måste göra är alltså att leta upp vilka paragrafer i *offentlighets- och sekretesslagen* som skulle kunna gälla för just den uppgift som du tror är skyddsvärd. När det gäller uppgifter som rör krisberedskap och totalförsvar kan det till exempel vara 15 kap. 2 §, 18 kap. 8 § eller 18 kap. 13 § OSL. Men inom dricksvattenområdet kan uppgifter också omfattas av flera andra sekretessbestämmelser, till exempel sekretess för affärs- och driftförhållanden eller för uppgifter som rör upphandling.

15 kap. 2 § offentlighets- och sekretesslagen

Enligt 15 kap. 2 § första stycket OSL kan sekretess gälla för uppgifter som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret.

[56] 2 kap. 2 § TF.

Totalförsvar består av militärt försvar och civilt försvar.[57] Ett av målen med det civila försvaret är att ha förmåga att upprätthålla en nödvändig försörjning. Totalförsvars-propositionen för 2021–2025 anger att dricksvattenförsörjning är en kritisk förutsättning för totalförsvaret som stöttar det civila försvarets samtliga förmågor.[58] Att uppgifter om dricksvattenförsörjning rör totalförsvaret har också fastslagits av domstol.[59]

18 kap. 8 § offentlighets- och sekretesslagen

Enligt 18 kap. 8 § OSL kan sekretess gälla för uppgifter som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd och åtgärden avser till exempel byggnad eller andra anläggningar, telekommunikation eller system för automatiserad behandling av information.

Inom dricksvattenförsörjningen kan sekretess gälla för uppgifter som rör en säkerhets-åtgärd, till exempel ritningar över larminstallationer[60], funktioner för användning av lösenord, loggning och kryptering, installation av brandväggar och antivirusprogram samt administrativa rutiner för till exempel utdelning av lösenord[61]. Sekretess kan också gälla för uppgifter som rör en bevakningsåtgärd, till exempel instruktioner och tjänstgöringslistor som rör bevakningen av en byggnad[62] eller bevakning av loggar och larm[63]. Bestämmelsen är även formulerad så att nedgrävning av ledning kan anses vara en säkerhetsåtgärd för att förebygga exempelvis skadegörelse.

Observera att sekretess enligt 18 kap. 8 § OSL **enbart** gäller uppgifter som rör antingen en säkerhetsåtgärd eller en bevakningsåtgärd. Den kan inte användas på andra typer av uppgifter.

18 kap. 13 § offentlighets- och sekretesslagen

Enligt 18 kap. 13 § OSL kan sekretess gälla för uppgifter som hänför sig till en myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida

---

[57] 1 § 3 st. lagen (1992:1403) om totalförsvar och höjd beredskap.

[58] Prop. 2020/21 s. 89 och s. 143.

[59] T.ex. RÅ 1989 not. 72 och mål nr 2828-2829–20 meddelad av Kammarrätten i Sundsvall den 30 november 2020.

[60] Prop. 1993/94:165 s. 18.

[61] Prop. 2003/04:93 s. 81 f.

[62] RÅ 1994 not 110 och RÅ not 111.

[63] Prop. 2003/04:93 s. 81 f.

krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer.

Bestämmelsen går att använda på uppgifter som har samlats in eller producerats inom ramen för analys-, planerings- eller förberedelseverksamheten avseende fredstida kriser, till exempel grunder för nedprioriteringar, detaljer om var reaktionstiden är lång och var möjligheten att upptäcka en incident är låg eller listor över nyckelpersoner och dessa personers ansvarsområden vid en eventuell krissituation.[64] Det kan också vara uppgifter som uppkommer under en kris, till exempel stabers uthållighet, gränssättande tekniska faktorer eller beroendeförhållanden av vissa leverantörer.[65]

Tips!

När du hittar den eller de paragrafer i *offentlighets- och sekretesslagen* som du tycker passar är det bra om du läser mer om dem. Läs förarbeten eller domar som berör den sekretessgrunden. Då får du en bättre uppfattning om du verkligen kan använda bestämmelsen på det viset du tänker dig. Ta hjälp av en jurist om du inte vet var du ska hitta juridiska källor.

Vilken skada kan uppstå om uppgifterna röjs?

En viktig del i sekretessbedömningen är skadeprövningen. Det är den del där du ska bedöma vilken skada som kan uppstå om uppgiften lämnar din organisation, det vill säga röjs. För att kunna göra en skadeprövning måste du ha kännedom om vilken hotbild som finns i samhället. Du får inte sekretessbelägga uppgiften innan du har gjort en skadeprövning.

15 kap. 2 §, 18 kap. 8 § och 18 kap. 13 § OSL har alla ett så kallat rakt skaderekvisit. Det innebär att uppgiften är offentlig om man inte kan anta att ett utlämnande vållar skada. Det är alltså bara om du kommer fram till att ett utlämnande kan orsaka skada som du får sekretessbelägga uppgiften. Annars måste du lämna ut den.

När du ska använda en bestämmelse med rakt skaderekvisit behöver du inledningsvis inte fundera på om ett utlämnande av uppgiften skulle orsaka skada om du lämnar dem till exakt den personen som nu har frågat efter dem. I bedömningen ska du först fundera på om uppgiften är sådan att ett utlämnande **typiskt sett** kan orsaka skada för det

[64] Prop. 2004/05:5 s. 259 f.

[65] Prop 2008/09:152, s. 17 f

intresse som ska skyddas genom bestämmelsen. Om uppgiften till exempel rör totalförsvaret och lätt kan missbrukas kommer den i de flesta fall omfattas av sekretess. Men om det är en uppgift som typiskt sett är harmlös omfattas den normalt inte av sekretess.

Gäller frågan en uppgift som en annan myndighet har lämnat till er är det lämpligt att ta kontakt med den myndigheten.[66] och fråga vilken skada de bedömer skulle kunna uppstå vid ett röjande. Det är ofta ett bra stöd, men glöm inte att din organisation måste göra bedömningen själv och att det är er bedömning som kommer att prövas av en domstol om beslutet skulle överklagas.

Ibland kommer du fram till att uppgiften är sådan att det typiskt sett kan antas orsaka skada att lämna ut den. Då ska du sekretessbelägga uppgiften. Det gör du genom att stryka över uppgiften så att den inte syns innan du lämnar ut handlingen. Du kan också dölja uppgiften på andra sätt, men om du till exempel klipper bort den från handlingen måste det framgå tydligt att den har stått där och att en sekretessbeläggning av den är gjord.

I vissa fall kan du lämna ut uppgiften även om ett utlämnande typiskt sett kan orsaka skada. En grundprincip är att du inte får fråga om identitet eller syfte med begäran när någon begär ut en allmän handling.[67] Personen har alltid rätt att vara anonym. Om du däremot kommer fram till att en uppgift typiskt sett kan vålla skada om den lämnas ut kan du faktiskt få efterfråga identitet och syfte med begäran.[68] Det kan ju vara så att uppgiften inte kommer vålla skada i det enskilda fallet och då ska du lämna ut den. Ett exempel är personuppgifter, som väldigt sällan är sekretessbelagda mot personen de gäller. Samma sak gäller när du ska lämna ut uppgiften till en annan myndighet. Eftersom sekretessbestämmelsen också gäller hos den myndigheten kan du anta att utlämnandet inte vållar skada.[69] Läs mer om delning mellan myndigheter i avsnittet *Sekretessbedömning mellan myndigheter*.

Tänk på att den som frågar efter uppgiften inte måste svara på dina frågor. Den har rätt att fortsätta vara anonym, men får då inte ta del av de sekretessbelagda uppgifterna.

---

[66] Till exempel prop. 2004/05:5 s. 264.

[67] 2 kap. 18 § TF och till exempel JO 2018/19 s. 320.

[68] Prop. 1979/80:2 Del A s. 81.

[69] Till exempel prop. 2004/05:5 s.264 och Högsta förvaltningsdomstolen mål nr 1208–1210-21 dom 2021-12-22.

Tips!

Om du behöver fråga någon som vill ta del av en handling vem den är eller varför den vill ha uppgiften kan det vara bra att förklara för personen varför du ställer frågan. Var tydlig med att personen inte måste svara på dina frågor, men att du inte kan lämna ut de sekretessbelagda uppgifterna om den inte gör det. Du måste också vara noga med att inte framställa det som att personen kommer att få ta del av uppgiften om den anger vem den är eller varför den vill ha uppgiften. Det får inte uppfattas som ett ultimatum och svaren behöver ju inte innebära att du lämnar ut uppgiften.

15 kap. 2 § offentlighets- och sekretesslagen

När en uppgift kan omfattas av sekretess enligt 15 kap. 2 § OSL ska du i din skadeprövning bedöma om det kan antas att det skadar landets försvar eller på annat sätt orsakar fara för rikets säkerhet om uppgiften röjs.

Begreppet rikets säkerhet omfattar bland annat folkförsörjningen.[70] Dricksvatten-försörjning är en del av folkförsörjningen och röjande av vissa uppgifter om dricksvattenförsörjningen kan alltså orsaka fara för rikets säkerhet.

I din skadeprövning behöver du fundera på vad som kan hända om uppgiften lämnas ut. Det blir enklare om du diskuterar med en kollega. Kan ett utlämnande av uppgiften typisk sett vålla fara för rikets säkerhet? Skulle en främmande makt kunna använda uppgiften för till exempel omfattande sabotage eller spioneri? Eller kan den användas för att förhindra eller försvåra så stor del av dricksvattenförsörjningen att det kan påverka Sveriges möjlighet att uthärda ett krig? Eftersom det ska vålla fara för **rikets** säkerhet räcker det sannolikt inte att till exempel ett samhälle utan viktig verksamhet för landets totalförsvar står utan dricksvatten.[71] Du måste bedöma att det faktiskt påverkar Sverige på nationell nivå.

Om du bedömer att det inte skulle skada rikets säkerhet att lämna ut uppgiften medför det inte att du måste lämna ut den. Uppgiften kan vara sekretessbelagd enligt en annan bestämmelse, till exempel 18 kap. 8 § eller 18 kap. 13 § OSL.

[70] Prop. 1979/80:2 Del A s. 133.

[71] Kammarrätten i Sundsvall mål nr 2828-2829-20 dom 2020-11-30.

18 kap. 8 § offentlighets- och sekretesslagen

När en uppgift kan omfattas av sekretess enligt 18. kap 8 § OSL ska du i din skadeprövning bedöma om det kan antas att syftet med säkerhetsåtgärden eller bevakningsåtgärden motverkas om uppgiften röjs.

I din skadeprövning behöver du fundera på vad som kan hända om uppgiften lämnas ut. Det blir enklare om du diskuterar med en kollega. Kan ett utlämnande av uppgiften typisk sett motverka syftet med åtgärden som omfattas av sekretessbestämmelsen? Du ska utgå från den säkerhets- eller bevakningsåtgärd som är aktuell. Om det till exempel rör en uppgift om vilka lösenord er organisations datorer har måste du börja med att ställa dig frågan vad syftet med säkerhetsåtgärden att ha lösenord är. Om du kommer fram till att syftet är att ingen obehörig ska kunna logga in i era datorer blir följdfrågan om detta syfte motverkas om någon utanför er organisation har en lista på de aktuella lösenorden. Det kan också gälla till exempel ronderingsscheman för vakter eller byggnadstekniska detaljer som syftar till att skydda det som finns i en anläggning. Motverkas syftet med de säkerhets- och bevakningsåtgärderna av att uppgifter om dem lämnas ut? Exempelvis koordinater som visar ledningens eller ledningsrättens exakta läge kan omfattas av sekretess, om säkerhetsåtgärden att gräva ned ledningen motverkas om någon som vill sabotera ledningen känner till ledningens exakta läge.

Om du bedömer att det inte skulle motverka den aktuella säkerhetsåtgärden eller bevakningsåtgärden att lämna ut uppgiften medför det inte att du måste lämna ut den. Uppgiften kan vara sekretessbelagd enligt någon annan bestämmelse, till exempel 15 kap. 2 § eller 18 kap. 13 § OSL.

18 kap. 13 § offentlighets- och sekretesslagen

När en uppgift kan omfattas av sekretess enligt 18 kap. 13 § OSL ska du i din skadeprövning bedöma om det kan antas att det allmännas möjligheter att förebygga och hantera fredstida kriser motverkas om uppgiften röjs.

I din skadeprövning behöver du fundera på vad som kan hända om uppgiften lämnas ut. Det blir enklare om du diskuterar med en kollega. Kan ett utlämnande av uppgiften typisk sett motverka det allmännas möjligheter att förebygga och hantera fredstida kriser? När det gäller 18 kap. 13 § kan det till exempel gälla att uppgifterna kan komma att användas för brottslig verksamhet som inbrott, bedrägeri, skadegörelse, sabotage eller terrorhandlingar.

Om det till exempel rör en uppgift om var er organisation har ett beredskapslager med vitala reservdelar får du fråga dig vad en person utanför er organisation skulle kunna använda den uppgiften till. Skulle den uppgiften till exempel kunna leda till att någon gör ett inbrott eller saboterar utrustningen? Skulle det då i sin tur motverka det allmännas möjligheter att förebygga och hantera fredstida kriser?

Om du bedömer att det inte skulle motverka det allmännas möjligheter att förebygga och hantera fredstida kriser att lämna ut uppgiften medför det inte att du måste lämna ut den. Uppgiften kan vara sekretessbelagd enligt någon annan bestämmelse, till exempel 15 kap. 2 § eller 18 kap. 8 § OSL.

Lämna ut uppgift med förbehåll

Ibland finns det behov av att låta en person som frågar efter en handling få ta del av en uppgift trots att den är sekretessbelagd. Det kan till exempel gälla en person som ska gräva på en plats och därför måste få veta vad som finns i marken för att inte orsaka skada eller en person som ska skriva en uppsats som kräver att han eller hon får ta del av sekretessbelagda uppgifter.

Vid utlämnandet av den sekretessbelagda uppgiften till en enskild kan en organisation göra ett förbehåll som inskränker mottagarens rätt att hantera uppgiften[72]. Ett förbehåll kan till exempel innebära att uppgiften bara får användas för ett specifikt ändamål, att den ska förvaras på ett speciellt sätt, att den inte får kopieras, att den inte får lämnas vidare eller att den ska förstöras när den använts för det angivna ändamålet eller ett bestämt datum.

Ett förbehåll är inget avtal mellan den utlämnande organisationen och mottagaren. Det ska istället utformas som ett beslut och i det ska det framgå vem det riktar sig mot och vad förbehållet innebär. Förbehållet ska också dokumenteras.[73]

Observera att den enskilde kan överklaga[74] att handlingen har lämnats ut med förbehåll. Den som bryter mot ett förbehåll kan dömas för brott mot tystnadsplikt[75].

Beslut och överklagande

När du är klar med din sekretessbedömning kan du ha kommit fram till att vissa uppgifter är sekretessbelagda. Då ska du stryka över de uppgifterna, eller på annat sätt dölja dem, och lämna ut handlingen. När du lämnar ut handlingen ska du upplysa om att det går att få ett överklagbart skriftligt beslut.[76]

---

[72] 10 kap. 14 § OSL.

[73] Prop. 1979/80:2 Del A s. 350 f och SOU 1975:102 s. 232.

[74] 6 kap. 7 § 2 OSL.

[75] 20 kap. 3 § brottsbalken (1962:700).

[76] 6 kap. 3 § 3 st. OSL.

Om personen begär ett skriftligt beslut ska myndigheten fatta ett sådant. Beslutet ska innehålla en klargörande motivering där du anger vilka regler du har använt och vilka omständigheter som har gjort att du har fattat beslutet[77].

Den som får beslutet ska också få en så kallad besvärshänvisning[78] som informerar om hur personen som har fått beslutet gör för att överklaga beslutet. Beslutet överklagas till kammarrätten.[79] Om beslutet överklagas och du inte har skrivit en tillräckligt klargörande motivering kan domstolen återförvisa ärendet till din organisation. Du får då tillbaka ärendet och får göra en noggrannare bedömning eller skriva en mer klargörande motivering.

Tips!

Skriv en bra, tydlig och förklarande motivering från början. Förklara varför bestämmelsen eller bestämmelserna i *offentlighets- och sekretesslagen* du har valt har använts på uppgiften. Förklara också på vilket sätt ett utlämnande skulle kunna orsaka skada.

Det ska vara enkelt för personen som får beslutet att följa ditt resonemang och förstå beslutet. Det räcker till exempel inte med att kopiera lagtexten i sekretessbestämmelsen och skriva att den innebär att uppgiften är sekretessbelagd. Låt gärna en kollega läsa din motivering när den är klar. Då märker du om det är enkelt att följa ditt resonemang eller om du behöver formulera dig annorlunda.

Domstolsprövningar och sekretess

Det finns ibland en oro för att en sekretessbelagd uppgift automatiskt blir offentlig om den hamnar hos en domstol vid ett överklagande. Den oron är ogrundad. 15 kap. 2 §, 18 kap. 8 § och 18 kap. 13 § OSL är sådana bestämmelser som gäller hos alla myndigheter, alltså måste också domstolarna tillämpa dem i sin verksamhet. Men också uppgifter som egentligen enbart är skyddade hos en myndighet eller i en viss typ av verksamhet är skyddade vid överklaganden. Om ett beslut överklagas och en myndighet skickar över uppgifter som ligger till grund för beslutet och uppgifterna är sekretessbelagda hos den myndigheten ska domstolen tillämpa sekretessbestämmelsen som att den också gällde hos domstolen.[80]

---

[77] 32 § FL.

[78] 33 § FL.

[79] 6 kap.8 § OSL.

[80] 43 kap. 1–3 §§ OSL.

En domstol som prövar ett beslut om sekretessbeläggning kan komma fram till att myndigheten har gjort fel bedömning och att uppgifterna ska lämnas ut. Inte heller i sådana domar skriver domstolen ut vilka uppgifter det rör sig om. Domstolen brukar skriva att det åligger myndigheten att lämna ut uppgifterna.

Länkar

Offentlighets- och sekretesslagen (2009:400)

Förvaltningslagen (2017:900)

Lagen (1992:1403) om totalförsvar och höjd beredskap

Riksdagens ombudsmän (JO)

Brottsbalken (1962:700)

Säkerhetskyddsklassificerade uppgifter

Säkerhetsskydd syftar till att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spioneri, sabotage, terroristbrott och vissa andra brott som kan hota säkerheten. I säkerhetsskydd ingår också att skydda uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt *offentlighets- och sekretesslagen*, eller som skulle ha omfattats av den lagen om den varit tillämplig. Att kunna göra en sekretessbedömning är därför en förutsättning för att kunna bedöma om en uppgift är **säkerhetsskyddsklassificerad**.

Säkerhetsskyddsklassificerade uppgifter delas in i fyra säkerhetsskyddsklasser, utifrån vilken skada för Sveriges säkerhet som kan uppstå om de röjs.[81] Uttrycket Sveriges säkerhet tar sikte på sådant som är av grundläggande betydelse för Sverige. I detta ingår bland annat det militära och civila försvaret, den nationella ekonomin, de brotts-bekämpande myndigheterna, domstolarna och sådana leveranser av exempelvis livsmedel, elkraft, dricksvatten och drivmedel som är nödvändiga för samhällets funktionalitet på nationell nivå.[82]

För att bedöma vilken skada som kan uppstå för Sveriges säkerhet om uppgifterna röjs måste du fundera på vilka eventuella konsekvenser ett röjande kan få. Konsekvenser av ett röjande som framstår som helt orimliga ska inte beaktas. I stället för att utgå ifrån det värsta tänkbara scenariot bör bedömningen göras utifrån vad som är det värsta *rimliga*

[81] https://www.sakerhetspolisen.se/verksamheten/sakerhetsskydd.html.

[82] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd*, s. 16.

scenariot om uppgifterna röjs. Enligt samma princip bör du inte heller beakta vad som skulle hända om andra uppgifter skulle röjas vid samma tidpunkt. I annat fall riskerar indelningen i säkerhetsskyddsklasser att leda till att i princip samtliga uppgifter delas in i någon av de högre klasserna, vilket inte är syftet med lagstiftningen.

För att en uppgift ska delas in i en säkerhetsskyddsklass krävs att de negativa konsekvenserna vid ett röjande påverkar den **nationella** förmågan. Med nationell förmåga avses till exempel den nationella försvarsförmågan, den nationella elförsörjningsförmågan eller den nationella betalningsförmågan. För en VA-huvudman skulle det kanske kunna gälla uppgifter om dricksvattenförsörjning till en helt avgörande försvarsanläggning. Men det är sannolikt ganska få VA-huvudmän som hanterar uppgifter om dricksvattenförsörjning som är säkerhetsskyddsklassificerade.[83]

Säkerhetspolisen har samlad information, föreskrifter och vägledningar i säkerhetsskydd på sin webbplats. Där hittar du också information om du behöver vägledning när du ska genomföra en säkerhetsskyddad upphandling.

Tips!

Bedömningar om säkerhetsskydd och säkerhetsklass kan rimligtvis inte göras av en ensam handläggare. Om du tror att uppgifter kan vara säkerhetsskyddsklassificerade bör du ta hjälp av någon i din organisation som arbetar med sådana frågor.

Länkar

Offentlighets- och sekretesslagen (2009:400)

Säkerhetspolisens information, föreskrifter och vägledningar

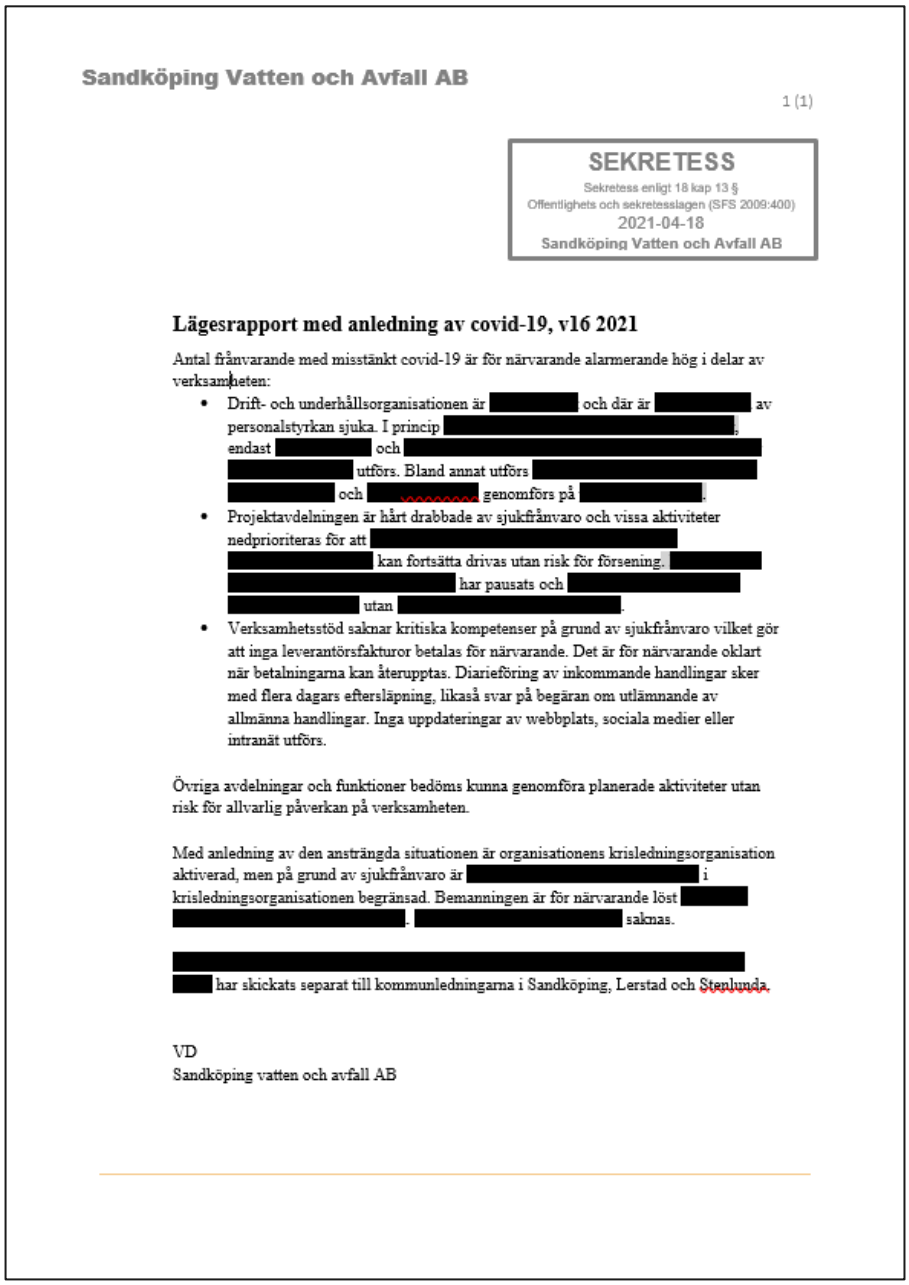
[83] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Informationssäkerhet,* s. 8 ff.

Exempel – utlämnande av allmän handling

Vid utlämnande av en allmän handling kan ett följebrev formuleras på följande sätt:

”Bifogat finns begärda handlingar. Vissa uppgifter har sekretessbelagts med stöd av X kap. X § offentlighets- och sekretesslag (2009:400) och du kan begära ett skriftligt överklagbart beslut.”

Handlingen lämnas ut med sekretessbelagda uppgifter maskade (se figur 1).



Sandköping Vatten och Avfall AB

1 (1)

SEKRETESS
Sekretess enligt 18 kap 13 §
Offentlighets och sekretesslagen (SFS 2009:400)
2021-04-18
Sandköping Vatten och Avfall AB

Lägesrapport med anledning av covid-19, v16 2021

Antal frånvarande med misstänkt covid-19 är för närvarande alarmerande hög i delar av verksamheten:

- Drift- och underhållsorganisationen är [redacted] och där är [redacted] av personalstyrkan sjuka. I princip [redacted], endast [redacted] och [redacted] utförs. Bland annat utförs [redacted] och [redacted] genomförs på [redacted].
- Projektavdelningen är hårt drabbade av sjukfrånvaro och vissa aktiviteter nedprioriteras för att [redacted] kan fortsätta drivas utan risk för försening. [redacted] har pausats och [redacted] utan [redacted].
- Verksamhetsstöd saknar kritiska kompetenser på grund av sjukfrånvaro vilket gör att inga leverantörsfakturor betalas för närvarande. Det är för närvarande oklart när betalningarna kan återupptas. Diarieföring av inkommande handlingar sker med flera dagars eftersläpning, likaså svar på begäran om utlämnande av allmänna handlingar. Inga uppdateringar av webbplats, sociala medier eller intranät utförs.

Övriga avdelningar och funktioner bedöms kunna genomföra planerade aktiviteter utan risk för allvarlig påverkan på verksamheten.

Med anledning av den ansträngda situationen är organisationens krisledningsorganisation aktiverad, men på grund av sjukfrånvaro är [redacted] i krisledningsorganisationen begränsad. Bemanningen är för närvarande löst [redacted], [redacted] saknas.

[redacted] har skickats separat till kommunledningarna i Sandköping, Lerstad och Stenlunda.

VD
Sandköping vatten och avfall AB

Figur 1. Exempel på allmän handling med sekretessbelagda uppgifter maskade.

Bilaga 2. Exempel – uppgifter inom dricksvattenförsörjning som kan omfattas av sekretess

Uppgifter inom dricksvattenförsörjning

Sekretessbedömning av uppgifter inom till exempel dricksvattenförsörjningen kan vara klurigt men det är ett hantverk som ryms i rollen som tjänsteman inom offentlig verksamhet. Förmåga att hantera uppgifter på rätt sätt balanserar allmänhetens behov av och rätt till insyn i offentlig verksamhet och behovet av att skydda känsliga uppgifter mot antagonister. Det är en mycket viktig arbetsuppgift som både värnar demokratin och stärker Sveriges totalförsvar.

Inom dricksvattenförsörjningen tillkommer ibland ytterligare hänsyn. I vissa situationer är det själva offentliggörandet av en uppgift som skyddar vattnet. Till exempel när det gäller vattenskyddsområden där människor som vistas i området måste veta hur de ska bete sig för att inte orsaka negativ påverkan på vattnet. Detsamma gäller skydd av ledningsrätter då skyddet uppstår först när åtgärden offentliggörs. När det gäller ledningsrätter är det viktigt att poängtera att offentliggörandet av själva åtgärden inte förutsätter att det exakta läget är offentligt.

Det är alltid aktören som förvarar en uppgift som bedömer uppgiftens skyddsvärde. Ingen annan myndighet eller organisation kan bestämma hur din organisation gör era bedömningar. När du bedömer skyddsvärdet ska du utgå från de rättskällor som finns.

För att underlätta arbetet med sekretessbedömningar inom dricksvattenförsörjningen har Livsmedelsverket tagit fram detta stöd med tips som ni kan använda i er bedömning. Observera att exemplen är just exempel och att uppgifterna inte alltid kommer att klassificeras på samma sätt av er. Ni måste *alltid* göra en egen bedömning i varje enskilt fall. Förhoppningsvis kan exemplen åtminstone tjäna som tankestöd i ert arbete eller vara ett underlag för den organisation som vill ta fram en egen, mer verksamhets-specifik, lista.

Alla bedömningar påverkas av den aktuella hotbilden vilket innebär att skrivningarna om olika uppgifter i texterna nedan tagits fram i en kontext. Det är viktigt att ni utgår ifrån det aktuella läget när ni gör era bedömningar om era uppgifter är skyddsvärda och omfattas av sekretess eller om de är öppna. Det kan också vara klokt att tänka efter innan uppgifter till exempel tillgängliggörs på en hemsida, även om de bedömts som öppna.

Sekretessbestämmelser

Listan nedan omfattar enbart sekretessbestämmelser i *offentlighets- och sekretesslagen* som rör krisberedskap och totalförsvar: 15 kap. 2 § (försvarssekretess), 18 kap. 8 § (säkerhets- och bevakningsåtgärd) och 18 kap. 13 § (risk- och sårbarhetsanalyser m.m.).

Tänk på att uppgifter inom dricksvattenområdet kan omfattas av flera andra sekretess-bestämmelser, till exempel sekretess för affärs- och driftförhållanden eller sekretess för uppgifter som rör upphandling. Ange alltid alla tillämpliga sekretessbestämmelser.

Sammanställning av exempel på uppgifter inom dricksvattenförsörjningen

Uppgifter om vattenverk

Exempel på uppgifter som kan vara öppna:

- verksamhetsområde och distributionsområde
- antal anslutna
- produktionsvolym
- intags- och uttagsvolym av råvatten
- namn på vattenverk, vattentäkt eller ID
- allmän beredningsinformation
- uppgifter om vattenkvalitet (rå- och dricksvatten).

Exempel på uppgifter som kan omfattas av sekretess:

- maxkapacitet för produktionsanläggning
- detaljerad beredningsinformation inklusive information om IT/OT-system
- information om processer för provtagning och mätning
- observationsrör och observationsbrunnar i anslutning till vattentäkt eller inom vattenskyddsområde
- delar av ritningar över anläggningar
- uppgifter om sårbarheter i processer och säkerhet.

Tips!

- Tänk efter före! När du skapar en handling kan det vara bra att tänka på om den kommer innehålla uppgifter som kan vara känsliga. Om den kommer att göra det kan du utforma handlingen så att den har en helt öppen del och en bilaga där alla känsliga uppgifter finns. På så sätt underlättar du för din organisation vid framtida delning eller publicering.
- Om du ska dela en handling med en annan myndighet kan det vara klokt att enbart skicka in de delar den myndigheten faktiskt behöver eller begär. På så sätt sprids inte uppgifter i onödan. Om du är osäker kan du alltid ringa och fråga vilken information de vill ha.
- Att en uppgift inte omfattas av sekretess innebär inte att den måste publiceras. Skilj på uppgifter som ni själva tillgängliggör till exempel på en hemsida och på uppgifter som ni måste lämna ut om någon begär det.

Geografiska lägen

Exempel på uppgifter som kan vara öppna:

- namn på vattenverk
- adress till vattenverk
- namn på ordinarie vattentäkter och reservvattentäkter.

Exempel på uppgifter som kan omfattas av sekretess:

- specifikt läge för intags- och uttagspunkter
- specifikt läge för ledning, servitut eller ledningsrätt.

Tips!

- Information om geografiska lägen som bedöms omfattas av sekretess kan sannolikt lämnas ut eller tillgängliggöras på annat sätt om de redovisas med mindre noggrannhet. Ett exempel kan vara att för ett geografiskt läge enligt koordinat-systemet SWEREF 99 TM ange de sista tre värdesiffrorna till 000. Detta innebär att en geografisk punkt istället anges utifrån en noggrannhet på cirka 1 km. Observera att en sådan noggrannhet inte alltid är lämplig, en bedömning måste alltid göras i varje enskilt fall. Fråga också den som vill ha uppgiften om den har nytta av den också med en sådan mindre noggrannhet. Det är viktigt att det framgår att en sådan åtgärd har vidtagits så att inte informationen används felaktigt.

Namn på vattenverk, vattentäkter (ordinarie och reservtäkter) samt adresser är sannolikt öppna uppgifter. I undantagsfall kan uppgifter om särskilt skyddsvärda anläggningar omfattas av sekretess.

Information om ledningsnätet

Exempel på uppgifter som kan vara öppna:

- begränsat område av ledningsnät
- att det finns en ledningsrätt (exakt läge kan ibland omfattas av sekretess).

Exempel på uppgifter som kan omfattas av sekretess:

- ledningar till skyddsvärda objekt
- ledningar där skada skulle ge omfattande negativa konsekvenser.

Tips!

- Det är vanligt att ägare av ledningar, kablar och annan infrastruktur använder sig av Ledningskollen för att balansera behovet av skydd mot att ledningar grävs sönder mot behovet av att skydda information om ledningsnätets exakta utformning i större områden. Det här är Ledningskollen.

Kartmaterial som visar ett begränsat område av ledningsnätet som inte angränsar till skyddsvärda objekt och inte inkluderar huvudledning eller annan ledning/objekt som vid avbrott skulle få omfattande negativa konsekvenser är sannolikt öppen information.

Information om driftsförhållanden

Exempel på uppgifter som kan vara öppna:

- översiktlig information om beredningsprocess
- personallistor med löner.

Exempel på uppgifter som kan omfattas av sekretess:

- detaljerad information om beredningsprocess
- bemanningsscheman för anläggningar som ibland är oövervakade
- personallistor som avslöjar en krisorganisation
- beskrivning eller utformning av kritisk IT/OT-infrastruktur.

Översiktlig information om beredningsprocessen i vattenverket är öppen. Men detaljerad information, inklusive information om IT/OT-system, kan sannolikt omfattas av sekretess.

Personallistor med befattningsbeskrivningar som ger information om dricksvattenförsörjningens krisorganisation kan omfattas av sekretess. Likaså kan driftinstruktioner som avslöjar när till exempel ett vattenverk är obemannat omfattas av sekretess. Uppgifter om samtliga anställdas lön är sannolikt öppna uppgifter.

Uppgifter om risker och sårbarheter

Exempel på uppgifter som kan vara öppna:

- övergripande beskrivningar av risker till exempel utmaningar med vattenbrist, kvalitetsproblem eller förnyelsebehov.

Exempel på uppgifter som kan omfattas av sekretess:

- vilka skyddsåtgärder som vidtagits
- vilka skyddsåtgärder som planeras, det vill säga sårbarheter som ännu inte åtgärdats
- vilka reservlösningar som finns
- var beredskapslager finns
- vilken kapacitet och uthållighet organisationen har vid kris och höjd beredskap.

Generellt är uppgifter om sårbarheter mer skyddsvärda än uppgifter om risker. Det är förmågan att hantera risker (eller inte) som måste skyddas. Det kan till exempel vara vilka säkerhets- och bevakningsåtgärder som har vidtagits, hur reservförfarande organiseras, vilken kapacitet och uthållighet man har till nödvattenförsörjning eller hur länge anläggningarna går att driva med reservkraft.

Information om vattentäkter

Exempel på uppgifter som kan vara öppna:

- namn på vattentäkter
- uppgifter som är straffsanktionerade.

Exempel på uppgifter som kan omfattas av sekretess:

- vilka säkerhets- och bevakningsåtgärder som vidtagits i närheten av vattentäkten
- känsliga lägen inom vattentäkten, till exempel uttagsbrunnar.

Namn på vattentäkter är sannolikt öppna uppgifter. Likaså uppgifter som är straff-sanktionerade. Det kan till exempel vara olika förbud som gäller inom ett område. Den som vistas där måste ha möjlighet att förstå att den bryter mot en regel om den planerar att vidta en åtgärd inom området. Känsliga geografiska lägen inom vattentäkten kan däremot omfattas av sekretess. Sekretess kan också gälla för säkerhets- och bevakningsåtgärder som har vidtagits för att skydda vattentäkten.

Bilaga 3. Exempel – intervjufrågor vid säkerhetsintervju

Det är en fördel att tillämpa någon form av mall för säkerhetsintervjun för att säkerställa att alla relevanta områden tas upp under samtalet. Nedan följer ett exempel på vilken typ av frågor som kan finnas i en intervjumall och som kan användas direkt eller anpassat efter den egna verksamhetens behov. Notera att en intervjumall för säkerhets-intervju aldrig ska fyllas i av den som prövas.

Under intervjun ställs frågor som kan upplevas som integritetskränkande. Det är därför viktigt att den som intervjuas får information om hur intervjun är tänkt att genomföras och att det är frivilligt att svara på frågorna (även om uteblivna svar såklart kan påverka bedömningen av säkerhetsprövningen). Kom ihåg att ta hänsyn till diskriminerings-grunderna[84] under intervjun.

Utgå aldrig från att personen som intervjuas är den han eller hon utger sig för att vara. Genomför därför en ID-kontroll i samband med säkerhetsintervjun.

Intervjufrågor

Tänk på att ställa följdfrågor utifrån den prövades berättelse samt fördjupa dig i områden där den prövade ger generella beskrivningar eller där du upplever att det finns oklarheter i berättelsen alternativt tänkbara sårbarheter.

[84] I lagen finns det sju diskrimineringsgrunder. Dessa är kön, könsöverskridande identitet eller uttryck, etnisk tillhörighet, religion eller annan trosuppfattning, funktionsnedsättning, sexuell läggning och ålder. Diskrimineringsgrunder – vad är det? | DO.

Livssituation och levnadsbakgrund

Skapa en tydlig bild av den prövades levnadsbakgrund och livssituation. Uppmärksamma problem och kriser i den prövades bakgrund och livssituation. Exempel på relevanta frågor:

- Hur ser familjesituationen ut? Gift, partner eller sambo?
- Egna barn eller barn från tidigare förhållanden?
- Bakgrund, uppväxt och skoltid?
- Fritidsintressen, engagemang, föreningsliv etc.?
- Konflikter inom familjen eller i släkten?
- Någon i familjen med annat medborgarskap, eller som bott utomlands?
- Någon i familjen som är brottsligt belastad?

Umgänge

Skapa en tydlig bild över den prövades umgängeskrets. Uppmärksamma problem och risker i den prövades umgängeskrets.

- Redogör för vänner och bekanta, begränsad eller omfattande umgängeskrets?
- Gamla vänner sedan länge eller nya?
- Deras sysselsättningar?
- Någon med brottslig belastning?
- Någon med speciella grupptillhörigheter som associeras med brottslighet?

Anställningar

Gå igenom den prövades anställningshistorik. Uppmärksamma särskilt tidsluckor och kortare anställningstider och undersök orsakerna till dessa. Försök bilda dig en uppfattning om hur den prövade har fungerat i tidigare anställningar – stämmer den förmedlade bilden med referenspersonernas bild? Notera även den prövades eventuella bisysslor. Bedöm om dessa kan innebära en konflikt med organisationens skyddsvärda intressen.

- Varit inblandad i konflikt på arbetsplatsen?
- Åsidosatt skyldigheter, ansvar eller uppgifter?
- Blivit utköpt av någon arbetsgivare, eller fälld i en personalansvarsnämnd?
- Eventuella bisysslor?

Exponering på internet

Diskutera den prövades exponering på internet som exempelvis sociala medier. Klargör om den prövade har förståelse för sårbarhet samt sekretess och vad som är lämpligt och olämpligt att publicera.

- Vilka sociala medier används?
- Används öppna profiler?
- Framgår arbetsplats och arbetsuppgifter i sociala medier?
- Vilken typ av information publiceras?
- Annan exponering på nätet?
- Medveten om hot och sårbarheter som finns på internet?

Alkohol och droger

Skapa en egen uppfattning om den prövades attityd och eventuella bruk av alkohol, droger och dopningsmedel. Var särskilt vaksam på om den prövade beskriver beteendeförändringar, negativa humörsvängningar eller minnesluckor i samband med alkoholförtäring eller om denne har blivit avvisad från fester eller offentliga lokaler på grund av alkoholförtäring. Då ska alkoholvanorna klargöras. Det kan även vara av intresse att få den sökandes bild om hur denne uppfattas av omgivning vid onyktert tillstånd: trött, flamsig, pratig (om arbete) eller provokativ/aggressiv.

- Egen alkoholkonsumtion?
- Har drickandet fått konsekvenser i privat- eller arbetsliv?
- Blivit avvisad från fester och offentliga lokaler eller omhändertagen för fylleri?
- Genomgått behandling för alkoholberoende?
- Attityd till narkotika och dopningsmedel?
- Brukat narkotika eller dopningsmedel, i så fall vad och hur ofta?
- Har bruk av narkotika eller dopningsmedel fått konsekvenser för privat- eller arbetsliv?
- Genomgått behandling för drogberoende?

Utlandsvistelser

Få en bild över den prövades resvanor, både privat och i arbetet.

- Vilka länder är intressanta resmål och varför?
- Vad är syftet med resorna?
- Har resor, privat eller i arbetslivet, resulterat i nya vänner eller bekanta?
- Vad vet den sökande om dessa?
- Andra utländska kontakter från utlandsvistelser?
- Bott utomlands under en kortare eller längre tid?
- Rest till konfliktområden?
- Haft kontakter med utländska myndigheter, ambassader, militär, polis eller personer kopplade till terrorism?

Utbildningar och licenser

Det kan vara av intresse att veta motivet till valet av mer ovanliga utbildningar eller licenser om det är kunskaper som inte har något med nuvarande eller tidigare yrkesval och/eller fritidssysslor att göra.

- Utbildningsbakgrund?
- Finns en röd tråd mellan utbildningar och anställningar?
- Körkort?
- Vapenlicens?
- Genomfört värnplikt?
- Säkerhetsutbildning, kunskap och förståelse för säkerhet och sekretess?
- Annan utbildning eller andra licenser?

Språk

Om den prövade har kunskaper i språk som inte vanligen lärs ut i svenska skolor är det relevant att fråga varför och var personen har fått dessa kunskaper. Har den prövade exempelvis kontakter eller andra relationer till personer i landet där det aktuella språket talas?

- Vilka språk behärskas?
- Var har språkkunskaperna förvärvats?

Brottslig belastning

Ett utfall i polisens register utesluter inte nödvändigtvis en anställning i tjänst placerad i säkerhetsklass. Det är dock kraftigt försvårande om förekomst i belastningsregister inte tagits upp vid säkerhetsprövningsintervjun men påträffas vid efterföljande registerkontroll. Det är viktigt att den prövade informeras om och förstår detta.

- Varit föremål för polisingripande?
- Involverad i verksamhet som kan betraktas som brottslig?
- Misstänkt för eller lagförd för något brott?
- Kontakt med kriminella grupperingar?

Ekonomi

Skaffa en så klar bild som möjligt av den prövades ekonomiska situation. Hur har den prövade hanterat sin ekonomi hittills och hur ser den ut i dag och i framtiden?

Visar den prövade att den inte har någon strategi för hantering av sin ekonomi, eller om det finns drag av girighet eller orealistisk ekonomisk livsföring, kan denne vara sårbar från säkerhetssynpunkt.

- Ekonomisk situation, inkomster och skulder?
- Delad ekonomi inom familjen?
- Fastighetsinnehav?
- Övriga tillgångar?
- Underhållsskyldighet?
- Antal krediter och hur stora?
- Betalningsanmärkningar eller skulder till kronofogden?
- Spel- eller köpberoende?
- Spel om pengar?

Lojalitet

Ta reda på om den prövade har släktband, yrkesmässiga eller nationella band till någon organisation, individ eller nation, som kan påverka dennes lojalitet mot arbetsgivaren och de intressen som ska skyddas med säkerhetsskyddslagen. Om sådana band finns, ta reda på om den prövade skulle uppleva det problematiskt att skydda sekretessbelagd information som skulle vara av stort värde för de som han eller hon har lojalitetsband till.

- Åtaganden eller intressen som särskilt engagerar?
- Lojalitetskonflikt med tidigare arbetsgivare?
- Tidigare hemland eller övriga band som kan innebära lojalitetskonflikt?

Efter intervjun görs en bedömning om något under intervjun kommit upp som kan anses påverka den prövades pålitlighet och lojalitet. Bedömningen dokumenteras.

Bilaga 4. Exempel – sekretess-förbindelse

Denna sekretessförbindelse gäller för anställda, praktikanter, elever inom arbetsplats-förlagd utbildning, inhyrd personal, entreprenörer, konsulter och förtroendevalda som kan komma i kontakt med uppgifter som omfattas av sekretess på Grusstads kommun, Teknik- och fastighetsförvaltningen.

Förbindelsen gäller för

Namn: _____ Personnummer: _____

Befattning: _____ Organisation: _____

Enhet: _____ Ansvarig chef: _____

Jag försäkrar att jag har tagit del av bifogad information om bestämmelserna i offentlighets- och sekretesslagen och förstått vad som gäller för mig utifrån mitt uppdrag.

Jag försäkrar att jag inte talar om eller på annat sätt för vidare sådant som jag får reda på om enskilda människors personliga förhållanden, tredje man, affärsförhållanden eller liknande som kan omfattas av sekretess. Jag har förstått att detta gäller för mig under den tid jag är verksam hos Grusstads kommun samt även för all tid därefter.

Jag är medveten om att överträdelse av dessa förbindelser kan medföra straffansvar, skadeståndsskyldighet och arbetsrättsliga åtgärder.

Förbindelse

Jag bekräftar härmed att jag erhållit information om offentlighets- och sekretesslagen och förbinder mig att följa ovanstående regler vad gäller sekretess.

_____	_____	_____
Datum	Namnteckning	Namnförtydligande

Denna förbindelse skrivs under i två exemplar. Varav parterna tar var sitt.

Jag har idag, med anledning av att min anställning kommer att upphöra, informerats om den tystnadsplikt som gäller för uppgifter som omfattas av sekretess och som jag fått del av i samband med anställningen.

_____	_____	_____
Datum	Namnteckning	Namnförtydligande

Bilaga 5. Exempel – Sandköping vatten och avfall AB:s tillträdesrutin

Anställda

Anställd personal inom Sandköping vatten och avfall AB har bara tillgång till de anläggningar som krävs för att kunna utföra sitt arbete. Normalt tillträde är vardagar 06:30–18:00, men beredskapspersonal har tillträde dygnet runt. Vid arbete i yttre anläggningar ska ankomst till anläggningen alltid meddelas till Sandköping vatten och avfalls driftcentral, likaså innan platsen lämnas efter utfört arbete.

Entreprenörer och konsulter

Entreprenörer och konsulter som ska utföra arbete i Sandköping vatten och avfalls lokaler ska ha en ansvarig kontaktperson från Sandköping vatten och avfall, normalt den som beställt arbetet. För att utföra arbete självständigt i lokalerna krävs erforderlig hygienutbildning och genomgång av verksamhetens säkerhetsföreskrifter, i annat fall krävs att kontaktpersonen övervakar arbetet. För arbete i skyddsobjekt krävs även genomförd säkerhetsutbildning och sekretessförbindelse. Vid arbete i yttre anläggningar ska ankomst alltid meddelas till Sandköping vatten och avfalls driftcentral, likaså innan platsen lämnas efter utfört arbete.

Entreprenörer och konsulter som utför arbete i vattenverket eller på huvudkontoret ska använda besökssystemet för att anmäla när de anländer respektive lämnar platsen. Besöksbrickan med namn, organisation, datum och ankomsttid ska bäras väl synlig under pågående arbete.

Hyresgäster

Särskilda tillträdesregler tillämpas för hyresgäster och deras underentreprenörer i Stenbergsreservoaren. Vid varje tillträdestillfälle ska hyresgästen kontakta Sandköping vatten och avfalls vaktbolag för ledsagning med skyddsvakt. Endast personer som föranmälts som behöriga av hyresgästen och som Sandköping vatten och avfall godkänt och meddelat vaktbolaget är behöriga att beställa ledsagning och därmed få tillträde till anläggningen. Skyddsvakt meddelar Sandköping vatten och avfalls driftcentral innan tillträdet, kontrollerar giltig ID-handling, är med och övervakar hela arbetet, säkerställer att anläggningen låses och larmas efter avslutat arbete och kontaktar driftcentralen på nytt innan platsen lämnas.

Besökare

Alla som inte är anställda, entreprenörer, konsulter eller hyresgäster betraktas som besökare. Det kan vara till exempel myndighetsrepresentanter, leverantörs-representanter, forskare, konsulter, utbildare, kandidater för tjänster, representanter från olika samverkansparter eller studiebesökare. Besökare ska ha en utsedd besöks-mottagare som är anställd på Sandköping vatten och avfall. Besökare får inte röra sig fritt i anläggningarna utan ska följas av sin besöksmottagare under hela besöket.

Besök på Sandköping vatten och avfalls anläggningar ska endast tillåtas i de fall det finns ett verksamhetsrelaterat syfte med besöket. Särskild restriktivitet ska gälla besök vid skyddsobjekt. Då utländska besök i vissa fall kan utgöra en större risk ur säkerhetsskyddsperspektiv ska sådana besök alltid på förhand anmälas till och godkännas av säkerhetschef.

Åldersgräns för besök i den operativa verksamheten är 16 år.

Alla besökare till vattenverket eller huvudkontoret ska använda besökssystemet för att anmäla när de anländer respektive lämnar platsen. Besöksbrickan med namn, organisation, datum och ankomsttid ska bäras väl synlig under hela besöket.