MittSverige Vatten&Avfall

Innehållstyp
Riktlinje

Dokumentnummer
1400640

Version
4.0

Godkänd av
Wikner Anneli

Godkänt datum
2022-06-20

Säkerhetsklass
1

# Allmänna och säkerhetsklassade handlingar

# Innehållsförteckning

1 Inledning ..... 1
2 Allmänna handlingar ..... 1
2.1 Detta är en handling ..... 1
2.1.1 Detta är en allmän handling ..... 2
2.1.2 Detta är inte en allmän handling ..... 2
2.2 Sekretessbelagd handling ..... 3
3 Säkerhetsklassificering av information ..... 3
3.1 Bedömning av säkerhetsklass ..... 3
3.1.1 Säkerhetsklass 0 ..... 4
3.1.2 Säkerhetsklass 1 ..... 4
3.1.3 Säkerhetsklass 2 ..... 4
3.1.4 Säkerhetsklass 3 ..... 5
3.1.5 Säkerhetsklass 4 ..... 6
4 Hanteringsregler ..... 7
4.1 Generella hanteringsregler för säkerhetsklass 1-3 ..... 7
4.2 Säkerhetsklass 1 ..... 7
4.3 Säkerhetsklass 2 ..... 8
4.4 Säkerhetsklass 3 ..... 8
4.5 Säkerhetsklass 4 ..... 9
4.5.1 Begränsat hemlig och konfidentiell information ..... 9
4.5.2 Hemlig och kvalificerat hemlig information ..... 10
5 Sekretessbedömning ..... 11
5.1 Sekretess i samband med upphandling ..... 11
5.2 Sekretessmarkering ..... 12
6 Utlämnande av allmän handling ..... 12
6.1 Krav på skyndsam handläggning ..... 12
6.2 Formerna för utlämnande ..... 12
6.3 Rätt till anonymitet ..... 13
6.4 Sekretessprövning och sekretessbeslut ..... 13
7 Delning av information till andra aktörer ..... 14
7.1 Sekretessbrytande bestämmelser ..... 14

7.2 Inför delning av information till andra aktörer ..... 14
7.2.1 Godtagbara skäl för att dela skyddsvärd information ..... 14
7.2.2 Delning till leverantörer ..... 14
7.2.3 Delning till myndigheter ..... 16
7.2.4 Delning av ledningsnätskartor utan affärsrelation ..... 16
7.3 Giltighetstid för sekretessförbindelser och intyg om säkerhetsprövning ..... 16
8 Brott mot tystnadsplikt och tjänstefel ..... 16
9 Bilagor ..... 17

# 1 Inledning

MittSverige Vatten & Avfall (MSVA) är ett kommunalt bolag och ska därför tillämpa offentlighetsprincipen. Offentlighetsprincipen ger allmänhet och massmedia rätt till insyn i det allmännas verksamhet, vilket bland annat omfattar rätten att ta del av allmänna handlingar. Det finns dock vissa begränsningar i rätten att ta del av allmänna handlingar.[1]

Med stöd av offentlighets- och sekretesslagen (OSL) kan vissa typer av uppgifter beläggas med sekretess, vilket innebär att uppgifterna omfattas av tystnadsplikt. Tystnadsplikten innebär ett förbud mot att röja uppgiften till obehöriga oavsett om det sker muntligen, genom att en handling lämnas ut eller på annat sätt.

En formell sekretessbedömning genomförs normalt sett först när en handling begärs ut. För att vi ska kunna hantera information på rätt sätt fram till dess ska all information värderas och klassificeras. Vid en fullständig informationsklassificering bedöms aspekterna konfidentialitet, riktighet och tillgänglighet. I denna riktlinje behandlas enbart konfidentialitet eftersom det är den aspekt som har en direkt koppling till sekretess enligt OSL.

Riktlinjen ger information om:

- offentlighetsprincipen och vad en allmän handling är
- klassificering av information i olika säkerhetsklasser och kopplingen till sekretess
- hanteringsregler för olika säkerhetsklasser
- handläggning av en begäran om att ta del av handlingar inkl. sekretessbedömning
- delning av säkerhetsklassad information till andra aktörer

Riktlinjen och tillhörande bilagor ska användas när dokument upprättas och ändras samt inför och vid delning eller utlämning av information eller handlingar.

# 2 Allmänna handlingar

## 2.1 Detta är en handling

Allt som innehåller någon form av information, oavsett medium, är att betrakta som en handling.[2] Det kan handla om pappersdokument, bilder, band- och videoupptagningar, sms, e-post eller annan digital information som förvaras på USB-minnen, hårddiskar eller liknande.

[1] 2 kap §§ 1-2 Tryckfrihetsförordningen (TF)
[2] 2 kap § 3 TF

### 2.1.1 Detta är en allmän handling

En handling är allmän om den förvaras hos en myndighet och antigen har inkommit till myndigheten eller har upprättats där.[3] Kommunala bolag likställs i detta fall med en myndighet.[4]

En handling är inkommen när den har anlänt till våra lokaler oavsett hur. En handling kan också vara inkommen om den har lämnats till en medarbetare utanför lokalerna, till exempel på ett externt möte eller liknande. Det finns inget krav på att en handling ska vara läst eller registrerad för att den ska anses som inkommen. Det innebär att ett e-postmeddelande som tillhör tjänsten anses inkommit så snart det ligger i inkorgen, oavsett om det är öppnat eller inte. Det är därför viktigt att det finns rutiner för att öppna och ta hand om e-post och post vid medarbetares frånvaro. Frånvaromeddelande på e-posten fungerar som information för mottagaren men fritar oss inte från ansvaret att öppna och ta hand om e-posten.

En handling som är upprättad hos MSVA blir allmän när den är färdigställd eller har skickats utanför bolagets gränser.

Nya sammanställningar av datorlagrat material är en potentiell handling. En förutsättning för att det ska räknas som en allmän handling är att sammanställningen kan göras med rutinbetonade åtgärder, det vill säga med en begränsad arbetsinsats som inte medför nämnvärda kostnader. E-postloggar, cookiefiler[5] och globalfiler[6] är enligt praxis att betrakta som upprättade allmänna handlingar.

### 2.1.2 Detta är inte en allmän handling[7]

Utkast, ”kladdar”, koncept och annat underlag som ännu inte har färdigställts eller skickats till någon utanför MSVA är att betrakta som arbetsmaterial och är inte allmänna handlingar. Anbud är inte heller en allmän handling förrän tidsfristen för anbud har gått ut.

Handlingar som till sitt innehåll är rent privata är inte allmänna handlingar även om de skulle ha skickats till MSVA. Du bör dock undvika att blanda privat post med arbetsrelaterad post. Det innebär att du inte ska skicka arbetsrelaterad post från din privata e-post, att du inte bör skicka e-post med privat innehåll från din MSVA-adress och inte ange din MSVA-adress som kontaktväg i privata sammanhang.

Facklig post, det vill säga information som lämnas från en facklig organisation till ett platsombud på arbetsplatsen är inte allmänna handlingar.

Handlingar som inte är allmänna omfattas inte av offentlighetsprincipen och behöver inte lämnas ut.

---

[3] 2 kap. 3 § TF
[4] Kommunala bolag likställs i detta fall med myndigheter enligt 2 kap. 3 § OSL
[5] Filer som innehåller information om vilka webbsidor en användare har besökt
[6] Upptagningar som visar adressuppgifter över de hemsidor en användare har besökt på Internet
[7] 2 kap. TF

## 2.2 Sekretessbelagd handling

Allmänna handlingar är som huvudregel offentliga. Det stora flertalet allmänna handlingar på MSVA är offentliga och omfattas inte av sekretess. Det finns dock vissa typer av allmänna handlingar och uppgifter som kan omfattas av sekretess enligt OSL, se kapitel 5 Sekretessbedömning för mer information om sekretess.

# 3 Säkerhetsklassificering av information

Vid en fullständig informationsklassificering bedöms aspekterna konfidentialitet, riktighet och tillgänglighet. I denna riktlinje behandlas enbart konfidentialitet eftersom det är den aspekt som har en direkt koppling till sekretess enligt OSL. För mer information om övriga aspekter se MSVA:s Instruktion för informationsklassning och riskanalys (Bilaga 10).

För att avgöra informationens säkerhetsklass använder MSVA en klassificeringsmodell med fem klasser. Säkerhetsklassning ska genomföras för all information, exempelvis i samband med att ett dokument upprättas och när innehållet ändas på ett sätt som kan påverka klassningen. Alla internt upprättade handlingar ska märkas med aktuell säkerhetsklass i sidhuvudet eller på annan lämplig plats (0, 1, 2, 3 eller 4).

Den interna säkerhetsklassningen anger vilket skydd informationen kräver och hur informationen ska hanteras. För att kunna avslå en begäran om att ta del av en allmän handling måste dock uppgifter också kunna beläggas med sekretess enligt OSL.

## 3.1 Bedömning av säkerhetsklass

Utgångspunkten för säkerhetsklass är en bedömning av skadan (konsekvensen) som kan inträffa om obehöriga tar del av information. För att undvika att stora mängder information klassificeras för högt ska orimliga konsekvenser inte beaktas. Av samma skäl ska bedömningen av enskilda uppgifter inte heller omfatta vad som kan hända om annan information röjs vid samma tillfälle.

I vissa fall kan en konsekvens uppstå enbart på grund av att uppgifter kommer ut oavsett om det finns någon intention att orsaka skada eller inte. Det kan till exempel röra känsliga personuppgifter eller uppgifter kopplat till anbud i samband med en upphandling.

I andra fall krävs det också att den som fått ta del av informationen använder den för att orsaka skada, begå brott och/eller genomföra förberedelser för sabotage, terrorism eller krig. Det kan exempelvis röra sig om kartmaterial, risk- och sårbarhetsanalyser, beskrivningar av skalskydd och driftinstruktioner. I dessa fall är det viktigt att analysera vad uppgifterna skulle kunna användas till av någon som har kunskap, förmåga och intention att orsaka skada för att kunna bedöma konsekvenserna.

Nedan ges en beskrivning av säkerhetsklasser med exempel på vilken typ av information som kan placeras i olika säkerhetsklasser. Notera att exemplen är vägledande för att ge stöd till bedömningen och inte en fastställd lista på information i respektive säkerhetsklass. För ytterligare

stöd i bedömning av säkerhetsklass och sekretess kopplat till ledningsnätskartan finns en särskilt vägledning, se bilaga 7 Vägledning för bedömning av säkerhetsklass och sekretess i kartan.

### 3.1.1 Säkerhetsklass 0

Avser allmän och öppen information. Informationen omfattas inte av sekretess och innehåller inga personuppgifter. Ingen negativ påverkan eller enbart en försumbar skada kan uppstå om informationen sprids.

### 3.1.2 Säkerhetsklass 1

Informationen omfattar uppgifter av intern karaktär, endast allmänna offentliga handlingar och är inte skyddsvärd och innehåller enstaka personuppgifter av ej känslig karaktär. Det kan vara:

- arbetsmaterial
- kartmaterial som försörjer enskilda icke-skyddsvärda fastigheter med upp till 200 m dricksvattenledning
- uppgifter om brister eller fel som inte rör skyddsvärd verksamhet (vår förmåga att bedriva samhällsviktig verksamhet)
- enstaka personuppgifter

Att obehöriga tar del av informationen kan orsaka måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. Det kan handla om en måttlig ekonomisk förlust, att enstaka kunder uttalar sig negativt om oss i sociala medier eller att det blir en mindre notis i lokalpress. Det kan också innebära att vi får ett måttligt produktionsbortfall, behöver göra vissa omprioriteringar av verksamhet och får måttliga återställningskostnader i tid och pengar eller annan måttlig påverkan.

Enskilda individer kan notera störningen eller uppleva lindriga besvär, hot eller kränkningar men det uppstår inga personskador.

### 3.1.3 Säkerhetsklass 2

Informationen består av arbetshandlingar eller allmänna handlingar som kan bli föremål för sekretess enligt OSL. Information avsedd för internt bruk eller innehåller personuppgifter enligt GDPR. Det kan vara:

- ritningar över enstaka byggnader knutna till avfall och återvinning, avloppsreningsverk eller mindre betydelsefulla dricksvattenanläggningar där placering av larm och övriga säkerhetsåtgärder framgår
- kartmaterial som visar upp till 1 500 m ledningsnät över dricks- och spillvatten, utan särskilt skyddsvärda objekt
- uppgifter om enskilda säkerhetsrutiner
- ritningar plus tekniska beskrivningar
- drift- och skötselinstruktioner
- enskilda handlingsplaner vid störningar
- handlingar kopplat till systemet för styrning- och övervakning

- personuppgifter eller mer skyddsvärda personuppgifter som personnummer

Att obehöriga tar del av informationen innebär en betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. Den drabbade verksamheten kan fullfölja sina uppdrag men det finns en risk för kännbar påverkan, exempelvis en betydande ekonomisk förlust och/eller genom att det finns behov av att vidta extraordinära åtgärder.

Det kan handla om att vi lyfts fram på ett negativt sätt i både lokal- och riksmedier eller att mer organiserade grupper uttrycker missnöje i sociala medier. Missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande.

Andra myndigheter och organisationer kan påverkas. Samhällsviktiga funktioner i egen eller annan organisation påverkas men prioriterade funktioner kan upprätthållas på en acceptabel nivå. Det kan handla om ett tillfälligt stort produktionsbortfall, otjänligt dricksvatten, höga återställningskostnader i tid och pengar och/eller stora omprioriteringar av verksamheten, betydande negativ påverkan på miljön eller annan betydande negativ påverkan.

Enskilda individer kan uppleva konsekvenser som stora besvär eller stor ekonomisk påverkan av störningen. Det kan handla om lindriga personskador eller allvarliga hot och kränkningar.

### 3.1.4 Säkerhetsklass 3

Informationen innehåller uppgifter som är föremål för sekretess enligt OSL, känsliga personuppgifter, andra områdesspecifika lagstiftningar, tystnadsplikt eller som antingen ger en helhetsbild eller ger detaljerad information kopplat till särskilt skyddsvärda anläggningar/verksamhet som till exempel civila skyddsobjekt. Det kan vara:

- detaljerade beskrivningar av uthållighet eller förmåga inom olika delområden, till exempel reservkraft
- HACCP:er eller andra dokument där brister i förmåga och sårbarheter för skyddsvärda anläggningar/verksamhet redovisas samlat
- uppgifter om larm och övriga säkerhetsåtgärder som ger en helhetsbild eller för särskilt skyddsvärda anläggningar
- handlingsplaner vid sabotage eller andra antagonistiska angrepp
- kartmaterial som visar mer än 1 500 m ledningsnät över dricks- och spillvatten och installationer, beskrivningar och datamodeller som kan ge en helhetsbild över hur vattenförsörjningssystemet fungerar
- kartmaterial som visar geografisk placering av skyddsobjekt och ledningsnätet i anslutning till dessa anläggningar
- företagets totala styr- och övervakningssystem
- känsliga personuppgifter, exempelvis information om hälsa

Att informationen sprids till obehöriga innebär en allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. Det skapar stora svårigheter för den drabbade organisationen och verksamheten kan inte fullfölja sina uppdrag. Det kan handla om en allvarlig ekonomisk förlust, mycket stora återställningskostnader eller att vi blir föremål för ihållande nyhetsbevakning i rikstäckande medier eller av organiserade grupperingar i sociala

medier. Nyhetsbevakningen rör inte bara enskilda händelser eller personer utan hela vår grundläggande kultur.

Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt och prioriterade funktioner kan inte upprätthållas. Det kan vara ett mycket stort produktionsbortfall som kan vara långvarigt, kräva omfattande omprioriteringar av verksamheten och/eller innebära mycket höga återställningskostnader i tid och pengar samt allvarliga skador på miljön eller annan allvarlig negativ påverkan. Individers liv och hälsa äventyras och det kan innebära svåra personskador eller dödsfall.

### 3.1.5 Säkerhetsklass 4

Avser uppgifter som omfattas av sekretess och som rör Sveriges säkerhet, så kallade säkerhetskyddsklassificerade uppgifter enligt säkerhetsskyddslagen. Typen av uppgifter som blir placerade i säkerhetsklass 4 är till stor del samma som för säkerhetsklass 3. För att handlingar ska bli inplacerade i säkerhetsklass 4 krävs det att uppgifterna rör säkerhetskänslig verksamhet. Det kan till exempel handla om viktiga dricksvattenanläggningar, processnätet eller totalförsvarsplanering oavsett verksamhetsområde. Utöver att uppgifterna ska röra säkerhetskänslig verksamhet ska också konsekvensen av att uppgiften röjs påverka Sveriges säkerhet.

Ett röjande av informationen kan ge konsekvenser som påverkar Sveriges säkerhet, till exempel genom att omfattande fara för liv och hälsa föreligger eller att samhällsviktiga funktioner slås ut för många människor och/eller under lång tid.

Skadan kan uppstå på grund av att verksamhet av betydelse för totalförsvaret påverkas negativt, att människor skadas eller dör eller att staten inte längre kan garantera medborgarnas säkerhet. Skadan kan också uppstå genom att förtroendet för statens förmåga att skydda människors liv och hälsa, samt förmågan att upprätthålla samhällets funktionalitet undermineras eller annan negativ påverkan på Sveriges säkerhet.

Informationen ska märkas med säkerhetsklass 4 och klassificeras i enlighet med säkerhetsskyddslagen (2018:585) 2 kap. 5 §. Märkning ska ske enligt OSL och med aktuell säkerhetsskyddsklass med utgångspunkt från den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen görs enligt följande:

- *kvalificerat hemlig* vid en synnerligen allvarlig skada,
- *hemlig* vid en allvarlig skada,
- *konfidentiell* vid en inte obetydlig skada, eller
- *begränsat hemlig* vid endast ringa skada.

Kontakta säkerhetsansvarig för stöd i bedömningen. För mer information se Säkerhetspolisens Vägledning säkerhetsskydd - Informationssäkerhet.

# 4 Hanteringsregler

Hanteringsreglerna gäller för handlingar eller uppgifter i respektive säkerhetsklass oavsett om det handlar om original eller kopior. Vid behov av avsteg från hanteringsreglerna för säkerhetsklass 1-3 ska beslut fattas av ansvarig chef på MSVA i samråd med säkerhetsansvarig. Inga undantag ges för säkerhetsklass 4.

När det gäller säkerhetsklass 0 finns det inga särskilda hanteringsregler eller begränsningar i hur informationen får spridas eller användas. Interna dokument ska dock märkas för att visa på att säkerhetsklassning har genomförts.

## 4.1 Generella hanteringsregler för säkerhetsklass 1-3

För att säkerställa att obehöriga inte tar del av skyddsvärd information ska:

- arbetsdatorn låsas när den lämnas utan uppsikt inom MSVA:s lokaler.
- Utanför MSVA:s lokaler ska dokument, datorer eller andra bärbara enheter förvaras under uppsikt eller låsas in.
- Motsvarande krav gäller för externa aktörer som hanterar MSVA:s information.
- Extern spridning av skyddsvärd information ska begränsas.
- Vid delning av skyddsvärd information ska åtgärder vidtas för att säkerställa att uppgifterna skyddas och hanteras på ett korrekt sätt. Se kapitel 7 Delning av information till externa aktörer för mer information.

Detta gäller vid aggregerad/stora informationsmängder

- En stor mängd med information (digitalt eller fysiskt) med säkerhetsklass 2 som sammantaget ger en helhetsbild som motsvarar säkerhetsklass 3 ska hanteras som säkerhetsklass 3
- En stor mängd med information (digitalt eller fysiskt) med säkerhetsklass 2 som inte ger ökad helhetsbild/kunskap ska fortsatt hanteras som säkerhetsklass 2

Anmäl detta till säkerhetsansvarig

- Inbrott i lokaler/utrymmen där skyddsvärd information förvaras,
- förlust av dator/iPad/telefon
- misstankar om att obehöriga kan ha tagit del av skyddsvärd information
- brott som begås mot MSVA alltid ska polisanmälas.

## 4.2 Säkerhetsklass 1

Det finns inga krav på begränsning av intern spridning av informationen inom MSVA.

- Uppgifterna ska behandlas och förvaras så att de skyddas mot obehöriga.
- Dokument ska inte ligga framme utan uppsikt i utrymmen där externa besökare har tillträde.
- Extern spridning bör begränsas och ska föregås av en sekretessbedömning.

- Uppgifter som inte bedöms omfattas av sekretess kan delas/lämnas ut och handlingar kan skickas med vanligt brev och öppen e-post.

Enskilda handlingar i säkerhetsklass 1 ska inte omfattas av sekretess.

## 4.3 Säkerhetsklass 2

Spridningen av informationen ska vara begränsad och enbart ske till personer som:

- har tillräckliga kunskaper om hanteringen av skyddsvärd information
- behöver uppgifterna för sitt arbete

Hantering av information i klass 2

- Fysiska handlingar ska hållas under god uppsikt eller förvaras i ett låst utrymme (skrivbordsskåp,hurts som bara behörig har nyckel till).
- Elektronisk förvaring ska ske så att endast behörig personal kan ta del av informationen, exempelvis genom behörighetsstyrning i system eller mappar.
- Informationen får inte lagras i datamedier utanför organisationens brandvägg/externt, till exempel på en privat dator. Molntjänst kan användas förutsatt att en riskanalys genomförts och att tjänsten uppfyller de krav på skydd som framgår utifrån fastställd riskanalys.
- Förvaring av information synligt i bil eller andra fordon utan uppsikt ska undvikas.
- För utskrift ska skrivare med behörighetsskyddad utskrift eller lokal skrivare inom synhåll från den som skriver ut dokumentet användas.
- För delning av information inom kommunkoncernen kan också information delas via det lokala nätverket genom att en mapp med begränsad behörighet upprättas på N: (gemensam).
- Information ska krypteras vid delning via e-post. Använd verktyget ”skicka stora filer” (https://filer.sundsvall.se) eller Secure Mejlbox (mejla SSG@msva.se för tillgång). För mer information om kryptering se bilaga 8 Skapa krypterade filer
- Information kan skickas via e-post internt inom Sundsvalls kommun, förutom till de bolag som lagrar e-posten på M365-servrar (Stadsbacken, Sundsvall energi, Logistikparken)
- Information ska skickas via rekommenderat brev.
- Möten, samtal eller telefonsamtal ska ske avskilt för att minska risken för att obehöriga tar del av informationen.

## 4.4 Säkerhetsklass 3

Spridningen av informationen ska vara starkt begränsad och enbart ske till personer som:

- har tillräckliga kunskaper om hanteringen av skyddsvärd information
- behöver uppgifterna för sitt arbete

Hantering av information i säkerhetsklass 3

- Fysiska handlingar ska hållas under god uppsikt eller förvaras inlåsta i ett utrymme som går att låsa och att endast behöriga har nyckeln/kod.

- Elektronisk förvaring ska ske så att endast behörig personal kan ta del av informationen, exempelvis genom behörighetsstyrning och åtkomst ska loggas. Detta görs i Mitten, Ymer, IDUS, Public360, EDP Future
- Informationen får inte lagras i datamedier utanför organisationens brandvägg/externt, till exempel på en privat dator. Molntjänst kan användas förutsatt att en riskanalys genomförts och att tjänsten uppfyller de krav på skydd som framgår utifrån faställd riskanalys.
- Informationen får inte förvaras i bil eller andra fordon utan uppsikt.
- Kopiering eller utdrag ur handlingar ska ske i så liten omfattning som möjligt. För utskrift ska nätverksskrivare med behörighetsskyddad utskrift (follow print) eller lokal skrivare inom synhåll från den som skriver ut dokumentet användas.
- För delning av information inom kommunkoncernen kan också information delas via det lokala nätverket genom att en mapp med begränsad behörighet upprättas på N: (gemensam).
- Information ska krypteras vid delning via e-post. Använd verktyget ”skicka stora filer” (https://filer.sundsvall.se) eller Secure Mejlbox (mejla ISG@msva.se för tillgång). För mer information om kryptering se bilaga 8 Skapa krypterade filer.
- Information kan skickas via e-post internt inom Sundsvalls kommun, förutom till de bolag som lagrar e-posten på M365-servrar (Stadsbacken, Sundsvall energi, Logistikparken)
- Om informationen skickas via brev ska rekommenderat brev med säkerhetskuvert användas
- Möten och samtal ska ske avskilt för att minska risken för att obehöriga tar del av informationen. Telefonsamtal bör undvikas.
- Dokument ska förstöras med dokumentförstörare eller lämnas i ett låst kärl för destruktion.

## 4.5 Säkerhetsklass 4

### 4.5.1 Begränsat hemlig och konfidentiell information

Spridningen av informationen ska vara mycket starkt begränsad och enbart ske till personer som:

- bedöms pålitliga ur säkerhetssynpunkt
- har tillräckliga kunskaper om säkerhetsskydd
- behöver uppgifterna för sitt arbete
- är inplacerade i säkerhetsklass (ej krav vid begränsat hemlig information)

Hantering av information i säkerhetsklass 4

- Fysiska handlingar, elektroniska handlingar, USB-minnen eller CD-skivor ska märkas med aktuell säkerhetsskyddsklass och diarienummer eller annan lämplig identifieringsuppgift.
- Allmänna handlingar ska registeraras i diariet med en anteckning om var den förvaras, om den gallrats eller kommit bort. Handlingen ska dock inte läggas in digitalt i Public360 eller i något annat diarieföringssystem som inte godkänts av MSVA. Om handlingen inte längre bedöms vara säkerhetskyddsklassificerad eller om säkerhetskyddsklassen ändras ska

detta noteras på handlingen, vem som fattat beslutet och datum. Är handlingen allmän ska ändringen också registreras i Public360.

- Fysiska handlingar, elektroniska handlingar eller lagringsmedium ska förvaras inlåsta i säkerhetsskåp. Skyddsnivån ska motsvara lägst SS 3492. Övrig tid ska handlingarna vara under ständig uppsikt.
- Uppgifterna får endast lagras på datorer som inte har möjlighet till internetanslutning och endast skrivas ut eller kopieras på skrivare som ej är uppkopplade mot nätverk.
- Kopiering eller utdrag ska ske i så liten omfattning som möjligt.
- Vid delning av handlingar med säkerhetsskyddsklassificerade uppgifter ska delningen och mottagare registreras. Muntlig delgivning eller visning behöver inte registreras.
- Säkerhetsskyddsavtal (SUA) ska upprättas om information i säkerhetsskyddsklass konfidentiell eller högre delas inom ramen för ett affärsavtal.
- Information får inte skickas med e-post eller delas muntligt via telefon
- Handlingar ska överlämnas personligen, vilket är att föredra om det är möjligt, eller skickas som rekommenderat brev i ett säkerhetskuvert. Kontrollera att säkerhetskuvertet inte är skadat, notera eller spara serienumret som finns på kuvertet och datum för när du skickar det samt mottagare för att möjliggöra spårning och verifiering. Kontakta gärna mottagaren innan informationen skickas för att utbyta information om serienummer och datum för distribution.
- När du tar emot en försändelse i någon form av säkerhetsförslutet engångsemballage ska du undersöka att emballaget inte uppvisar spår av manipulation, till exempel i förslutning, skarvar och svetssömmar. Om spår av manipulation upptäcks eller om serienumret inte stämmer överens med det som avsändaren eventuellt angett ska det utredas som en potentiellt säkerhetshotande händelse. Kontakta säkerhetsansvarig vid en sån händelse.
- Möten där uppgifter diskuteras ska ske i lokaler där riskreducerande åtgärder har vidtagits, exempelvis ska inga telefoner, läsplattor, datorer eller annan utrustning med möjlighet att ansluta till nätverk finnas i rummet.
- Handlingar och datamedier som inte längre används, och inte ska arkiveras, ska destrueras. Handlingar ska brännas eller strimlas i en dokumentförstörare med lägst säkerhetsklass 5, spånstorlek 15x1,2 mm eller mindre. Handlingar får inte lämnas i de låsta kärl för destruktion som finns på MSVA.

### 4.5.2 Hemlig och kvalificerat hemlig information

För hemlig och kvalificerat hemlig information tillkommer ytterligare hanteringsregler. MSVA bedöms i nuläget inte hantera information i någon av dessa säkerhetsskyddsklasser, men det kan inte uteslutas att det vid något enstaka tillfälle kan bli aktuellt. I dessa fall är det VD som fattar beslut om förvaring av handlingar. Vid kopiering, utdrag eller vid medförande utanför våra lokaler krävs medgivande från VD. Förutom delning av handlingar och utdrag ska också muntlig delgivning eller visning av information registreras. Allmänna handlingar och lagringsmedier ska inventeras årligen. Destruktion ska dokumenteras.

# 5 Sekretessbedömning

När handlingar begärs ut, ska delas eller bedöms kunna omfattas av säkerhetsskyddslagen, ska en sekretessbedömning enligt OSL genomföras. Utgångspunkten är att det är den som är närmast berörd som genomför sekretessbedömningen med stöd av denna riktlinje och tillhörande stöddokument för sekretessbedömning. Det kan vara den som upprättat handlingen, har tagit emot den eller den som normalt sett ansvarar för det sakområde som uppgifterna rör. Bedömningen sker med fördel i samråd med chef och/eller sakkunniga. Vid osäkerhet i bedömningen ska samråd ske med säkerhetsansvarig eller informationssäkerhetsansvarig.

Vid en begäran eller inför en delning av information ska alltid en sekretessbedömning genomföras oavsett om handlingen sedan tidigare är märkt med säkerhetsklass eller har en sekretessmarkering. En säkerhetsklassning eller sekretessmarkering ska dock fungera som en varningssignal och samråd ska, om möjligt, ske med den som genomfört sekretessmarkeringen. Om handlingen har sekretessmarkerats av en annan organisation bör du kontakta denna för samråd och stöd med bedömningen.

När du genomför en sekretessbedömning ska handlingen eller handlingarna granskas i sin helhet. Att en begäran om att ta del av en allmän handling ska hanteras skyndsamt innebär inte att handläggning och sekretessbedömning inte får ta tid om materialet är omfattande. Den som har begärt ut uppgifterna bör dock upplysas om detta och få en förväntad handläggningstid.

För att en uppgift ska kunna beläggas med sekretess måste det finnas en paragraf i OSL som är tillämplig. Efter att ha identifierat lämplig paragraf ska, i de allra flesta fall, en skade- eller menbedömning genomföras. Det innebär att man bedömer den skada som det kan innebära att uppgiften lämnas ut inom ramen för det område som den aktuella paragrafen omfattar. Det är alltså inte tillräckligt att en uppgift exempelvis rör planering för en fredstida krissituation enligt OSL Kap. 18 § 13 för att den ska kunna sekretessbeläggas. Det krävs också att man kan visa på/motivera att ett röjande av uppgiften kan antas påverka förmågan att hantera en kris negativt.

## 5.1 Sekretess i samband med upphandling

I en offentlig upphandling råder absolut sekretess fram tills den upphandlande enheten meddelat tilldelningsbeslut eller avslutat upphandlingen. Absolut sekretess innebär att uppgifter omfattas av sekretess utan krav på skade- eller menbedömning. Det betyder att inga uppgifter om de anbud som kommit får offentliggöras, exempelvis vilka och hur många leverantörer som lämnat anbud eller vilka priser och övriga villkor som lämnats. Man får heller inte vid en eventuell förhandling avslöja något om prisnivåer i konkurrenters anbud eller vilka konkurrenterna är till en viss anbudsgivare i syfte att pressa priserna i dennes anbud.

Då tilldelningsbeslut fattats eller alla anbud offentliggjorts, omfattas samtliga handlingar rörande upphandlingar av de vanliga reglerna om handlingars offentlighet och sekretess. Det innebär att offentlighetsprincipen gäller för uppgifter i sådana handlingar och att var och en som huvudregel har rätt att ta del av dem. Om någon begär ut handlingar i ett upphandlingsärende ska en sekretessbedömning genomföras, särskilt om en anbudsgivare har begärt sekretess på hela eller delar av sitt anbud.

Det totala priset i det vinnande anbudet anses normalt inte vara föremål för sekretess efter det att tilldelningsbeslutet offentliggjorts.

## 5.2 Sekretessmarkering

Om det finns uppgifter som omfattas av sekretess ska handlingen sekretessmarkeras på första sidan enligt nedan. Markeringen för sekretess används när en handling innehåller uppgifter som omfattas av sekretess enligt OSL. Om uppgifterna är säkerhetsskyddklassificerade ska både aktuell säkerhetsskyddsklassificering, det vill säga begränsat hemlig, konfidentiell, hemlig eller kvalificerat hemlig, och tillämplig paragraf i OSL anges. Stämplar finns i postrummet på Stuvarvägen.

SEKRETESS
enl. offentlighets- och sekretesslagen
(2009:400) …. kap …. §
Datum……..
MittSverige Vatten&Avfall

BEGRÄNSAT HEMLIG
Sekretess enl. offentlighets- och sekretesslagen
(2009:400) …. kap …. §
Datum……..
MittSverige Vatten&Avfall

Därefter ska nedanstående markering läggas in i sidhuvudet på samtliga efterföljande sidor.

SEKRETESS
Se anteckning sida 1

BEGRÄNSAT HEMLIG
Se anteckning sida 1

För elektroniska handlingar eller uppgiftssamlingar där formatet inte stödjer en anteckning enligt ovan kan anteckningen om sekretess/säkerhetskyddsklassificering i stället anges i filnamnet.

På säkerhetsskyddsklassificerade handlingar ska också antalet sidor och eventuella bilagor anges på första sidan. Fysiska handlingar i säkerhetsskyddsklassen hemlig och kvalificerat hemlig ska också förses med en anteckning om handlingens exemplarnummer.

# 6 Utlämnande av allmän handling

## 6.1 Krav på skyndsam handläggning

En begäran om att ta del av en allmän handling ska behandlas genast eller så snart som möjligt, normalt inom samma dag. Det innebär att alla enheter på bolaget måste vara bemannade under kontorstid så att en begäran kan hanteras skyndsamt. Semester, sjukdom eller hög arbetsbelastning är aldrig godtagbara skäl att dröja med handläggningen.

## 6.2 Formerna för utlämnande

Den som begär ut handlingen kan antingen välja att komma till oss och ta del av handlingen på plats eller få en kopia på handlingen. Vi har ingen skyldighet att lämna ut allmänna handlingar

elektroniskt, även om det kan vara lämpligt i vissa fall. Information som har lagrats digitalt kan lämnas ut i form av en utskrift.

Om en begäran är oklar är vi skyldiga att hjälpa den enskilde att komplettera eller precisera sin begäran så att den kan hanteras, samt att inom rimliga gränser göra de efterforskningar som krävs för att försöka identifiera vilka handlingar den enskilde begär.

För kostnad se MSVA:s Taxa för beställning av allmänna handlingar.

## 6.3 Rätt till anonymitet

Den som begär ut en allmän handling som är offentlig har en grundlagsskyddad rättighet att få vara anonym och behöver inte heller ange syftet med sin begäran. Uppgifter som är offentliga ska därför lämnas ut utan efterforskning. Om handlingen innehåller uppgifter som kan omfattas av sekretess får du dock efterfråga både namn och syfte som underlag till din prövning.

## 6.4 Sekretessprövning och sekretessbeslut

När någon begär ut en allmän handling eller en uppgift i en handling ska det alltid göras en sekretessprövning för att avgöra om den kan lämnas ut eller inte. Om den allmänna handlingen är offentlig ska den omedelbart lämnas ut. En handling som innehåller sekretessbelagda uppgifter ska lämnas ut i de delar som är offentliga. Om sekretessbelagda uppgifter behöver döljas i en handling ska dessa maskeras.

Om begärda uppgifter inte kan lämnas ut på grund av sekretess ska den som har begärt uppgifterna meddelas bedömningen och skälen till att handlingen eller delar av den inte kan lämnas ut. I samband med detta ska du också meddela den enskilde om att den har rätt till ett skriftligt avslagsbeslut. Av beslutet ska det framgå varför uppgifterna inte kan lämnas ut med motivering och en hänvisning till aktuellt lagrum i OSL. Det ska också framgå hur beslutet kan överklagas. Kontakta jurist för stöd med formulering av beslut. Avslagsbeslut fattas slutgiltigt av VD.

I vissa fall kan det vara aktuellt att lämna ut sekretessbelagd information till enskilda med ett förbehåll som mottagaren måste godta för att handlingen ska lämnas ut. Som tidigare nämnt räcker det inte med att uppgiften kan knytas till en paragraf i OSL för att den ska omfattas av sekretess, utan det krävs också att ett röjande kan innebära skada enligt den aktuella paragrafen. Att en uppgift lämnas ut, till exempel ett kartmaterial i samband med grävarbeten, behöver inte innebära någon skada under förutsättning att uppgifterna används som avsett och inte sprids vidare. I förbehållet ställs krav på hanteringsregler som att uppgifterna inte får spridas vidare, att handlingen inte får kopieras, att den ska förvaras på ett sätt så att ingen annan kan ta del av den och så vidare.

Se bilaga 1 Sekretessbedömning vid begäran om att ta del av allmän handling för mer information och bilaga 7 Vägledning för bedömning av säkerhetsklass och sekretess i kartan.

# 7 Delning av information till andra aktörer

Att sekretess gäller för en uppgift innebär att det är förbjudet att röja uppgiften oavsett om det sker muntligen eller genom att en handling lämnas ut. Det kan dock finnas skäl och stöd i lagstiftningen att lämna ut en uppgift trots att den omfattas av sekretess.

## 7.1 Sekretessbrytande bestämmelser

I OSL finns det ett antal sekretessbrytande bestämmelser[8] som ger oss rätt att lämna ut sekretessbelagda uppgifter. Förutom ett antal paragrafer som berör specifika situationer finns också en generalklausul. Klausulen innebär att sekretessbelagda uppgifter får lämnas till en annan myndighet om det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda.[9] Sekretessbrytande bestämmelser kan också gälla vid absolut sekretess.

Offentligt anställda omfattas även av en grundlagsskyddad meddelarfrihet. Det innebär att offentligt anställda har rätt att muntligt lämna sekretessbelagda uppgifter till journalister eller författare för publicering om inte annat anges i OSL. I dessa fall får inte arbetsgivaren utreda vem som lämnat uppgifterna.

## 7.2 Inför delning av information till andra aktörer

### 7.2.1 Godtagbara skäl för att dela skyddsvärd information

När MSVA delar skyddsvärd information till externa aktörer ska informationen antingen vara en förutsättning för att företaget ska kunna utföra ett uppdrag/leverera en tjänst som vi har beställt eller för att en myndighet ska kunna utföra sin uppgift. Ett annat godtagbart skäl är att informationen utgör underlag för att ta fram obligatorisk statistik.

Ytterligare tillfälle där det kan finnas återkommande behov av att dela skyddsvärd information är när andra aktörer som infrastrukturägare, konsulter eller entreprenörer har behov av information om vårt ledningsnät för till exempel projektering, planering eller genomförande av projekt.

Om inte något av dessa skäl föreligger ska inte information i säkerhetsklass 2 eller högre delas, under förutsättning att ingen sekretessbrytande paragraf i OSL är tillämplig. Inför delning av information i säkerhetsklass 3 eller högre ska samråd ske med ansvarig chef på MSVA.

### 7.2.2 Delning till leverantörer

För att MSVA ska dela skyddsvärd information till leverantörer ska sekretess och/eller informationssäkerhet finns med i avtalet mellan MSVA och leverantören. I avtalet förbinder sig leverantören att följa våra hanteringsregler och, vid behov, våra krav på företagets arbete med

[8] Kap. 10 §§ 1-28 OSL
[9] Kap. 10 § 27 OSL

informationssäkerhet. Det sistnämnda är aktuellt om företaget ska förvara och hantera information i säkerhetsklass 2 eller högre i sina lokaler och system.

För säkerhetsklass 2, 3 och 4 kan det också vara aktuellt att ställa krav på att företaget ska ha en säkerhetschef eller säkerhetsansvarig som kan vara vår kontaktperson i säkerhetsfrågor. Personen ska även ansvara för att genomföra säkerhetsprövningar av personer som ska delta i skyddsvärd verksamhet och/eller ta del av information samt för att berörda undertecknar en sekretessförbindelse. I de fall detta inte är lämpligt, till exempel vid avtal med fåmansföretag, genomförs detta i stället av MSVA.

För delning av information i säkerhetsklass 4 ska också krav på säkerhetsskydd ställas. I vissa fall kan det vara aktuellt att upprätta ett SUA-avtal mellan oss och leverantören. Med SUA-avtal avses säkerhetsskyddad upphandling med säkerhetsskyddsavtal som upprättas mellan oss och anbudsgivaren eller leverantören. Detta är ett krav enligt säkerhetsskyddslagen i de fall en upphandling omfattar säkerhetsskyddsklassificerade uppgifter på nivån konfidentiell eller högre och/eller innebär ett deltagande i säkerhetskänslig verksamhet på motsvarande nivå.

En upphandling och/eller ett avrop av en tjänst måste alltså föregås av en inventering och analys av vilken typ av information som leverantören kommer att ta del av inom ramen för uppdraget, i vilka säkerhetsklasser och om information i säkerhetsklass 2 eller högre ska förvaras i leverantörens lokaler/system eller inte. Inventeringen och analysen ligger till grund för kravställning gentemot leverantören vad avser sekretess, informationssäkerhet, säkerhetsprövningar och eventuell inplacering i säkerhetsklass.

De individer som ska ta emot skyddsvärd information i säkerhetsklass 2 eller högre ska ha undertecknat en sekretessförbindelse. Den som skriver under förbindelsen ska ha läst och förstått de hanteringsregler som gäller för den eller de säkerhetsklasser som är aktuella. För information om hanteringsregler till externa aktörer kan bilaga 6 Utdrag ur riktlinje Allmänna och säkerhetsklassade handlingar för information till leverantörer och andra externa intressenter.

För säkerhetsklass 2, 3 och 4 ska också personen bedömas som pålitlig ur säkerhetssynpunkt. Säkerhetsprövningen ska anpassas till aktuell säkerhetsklass och i vilken omfattning personen kommer att ta del av skyddsvärd information. För säkerhetsklass 3 och 4 ska ett skriftligt intyg på godkänd säkerhetsprövning upprättas. Se bilaga 9 Information om säkerhetsprövning till leverantörer och andra externa intressenter för mer information.

För delning av information i säkerhetsklass 4 ska också mottagaren ha gått en utbildning i säkerhetsskydd. Krav på inplacering i säkerhetsklass gäller enbart om informationen i säkerhetsklass 4 har säkerskyddklassificering konfidentiell eller högre.

Vid SUA-avtal och delning av konfidentiell information ska mottagarna vara inplacerade i säkerhetsklass och ha genomgått en utbildning i säkerhetsskydd.  I dessa fall är ett SUA-avtal en förutsättning både för att kunna dela information och för att kunna ställa krav på inplacering i säkerhetsklass.

### 7.2.3 Delning till myndigheter

Vid delning av information till myndigheter eller kommunala bolag som omfattas av OSL behöver vi inte avtala om hur informationen ska hanteras eller kräva att personer undertecknar en sekretessförbindelse. MSVA ska dock informera mottagaren om att vi bedömer att informationen är skyddsvärd och, i förekommande fall, om vilken paragraf i OSL som tillämplig samt vilka hanteringsregler vi förväntar oss att myndigheten ska följa. De personer som ska ta del av informationen ska ha kunskap om hantering av skyddsvärd och/eller sekretessbelagd information och bedömas vara pålitlig ur säkerhetssynpunkt. Myndighetens säkerhetschef eller säkerhetsskyddschef ska kontaktas vid behov för bedömning och intyg om godkänd säkerhetsprövning.

### 7.2.4 Delning av ledningsnätskartor utan affärsrelation

Även vid delning av ledningsnätskartor till aktörer som vi inte har någon egen affärsrelation till ska vi ställa krav på att mottagaren följer tillhörande hanteringsregler, att personer som tar del av information i säkerhetsklass 2 eller högre undertecknar sekretessförbindelser och bedöms pålitliga ur säkerhetsynpunkt. Är behovet av att ta del av ledningsnätskartor omfattande och/eller återkommande bör ett avtal som reglerar säkerhetskrav tecknas mellan MSVA och aktören. Vid övriga tillfällen ansvarar den som delar informationen för att kraven uppfylls. Kontakta säkerhetsansvarig vid behov av stöd.

## 7.3 Giltighetstid för sekretessförbindelser och intyg om säkerhetsprövning

Sekretessförbindelser och intyg om säkerhetsprövning kan antingen gälla för en ramavtalsperiod eller för ett enskilt uppdrag. För ramavtalsaktörer som återkommande genomför arbeten under hela avtalsperioden utan längre avbrott kan giltighetstiden anges till hela ramavtalsperioden, under förutsättning att angiven säkerhetsklass inte ändras eller att något som föranleder en ny säkerhetsprövning inte inträffar.

I de fall MSVA gör enstaka avrop för avgränsade uppdrag bör i stället sekretessförbindelser och intyg gälla för det aktuella uppdraget.

Kontakta säkerhetsansvarig vid behov av stöd i bedömningen av lämplig giltighetstid.

# 8 Brott mot tystnadsplikt och tjänstefel

Sekretess innebär att det är förbjudet att röja uppgiften oavsett om det sker muntligen eller genom att en handling lämnas ut. Den som röjer en sekretessbelagd uppgift kan dömas för brott mot tystnadsplikt under förutsättning att meddelarfrihet eller någon annan sekretessbrytande bestämmelse inte gäller. Detta gäller oavsett om det skett avsiktligt, på grund av slarv eller okunskap.

Den som medvetet eller av oaktsamhet sätter offentlighetsprincipen ur spel, exempelvis genom att vägra lämna ut offentliga handlingar, kan dömas för tjänstefel.

# 9 Bilagor

Följande stöddokument och blanketter utgör bilagor till denna riktlinje:

Bilaga 1 Sekretessbedömning vid begäran om att ta del av allmän handling

Biaga 2 Delning av information till företag

Bilaga 3 Delning av information till myndighet inkl. kommuner

Bilaga 4 Sekretessförbindelse

Bilaga 5 Blankett för delning av säkerhetsklassad information

Bilaga 6 Hanteringsregler säkerhetsklassad information, för externa aktörer

Bilaga 7 Vägledning för bedömning av säkerhetsklass och sekretess i kartan

Bilaga 8 Skapa krypterade filer

Bilaga 9 Information om säkerhetsprövning till leverantörer och andra externa intressenter

Bilaga 10 Instruktion för informationsklassning och riskanalys